(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/45453 A1

(51) International Patent Classification⁷: H04Q 7/38

(21) International Application Number: PCT/FI01/00870

(22) International Filing Date: 9 October 2001 (09.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20002613 28 November 2000 (28.11.2000) FI
20010282 14 February 2001 (14.02.2001) FI

(71) Applicants *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **NIEMI, Valtteri** [FI/FI]; Tallbergінkatu 3 as. 43, FIN-00180 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **VIALÉN, Jukka** [FI/FI]; Haltiantie 3 C, FIN-02300 Espoo (FI).

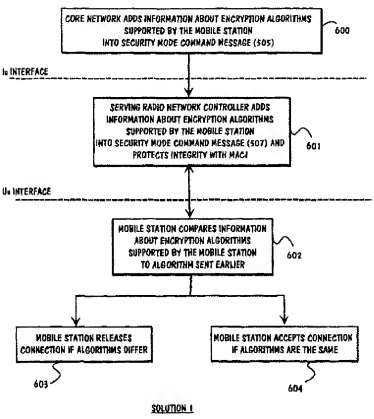
(74) Agent: **RUUSKANEN, Juha-Pekka**; Page White & Farrer, 10th floor, Runeberginkatu 5, FIN-00100 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) **Title:** A SYSTEM FOR ENSURING ENCRYPTED COMMUNICATION AFTER HANDOVER



SOLUTION 1

(57) Abstract: A fraudulent intruder can eavesdrop on a call by removing information about an encryption algorithm when a multimode mobile station sends an unpro-tected initial signaling message containing this information over the radio interface to the mobile telecommunications system. The attempt can be pre-vented in a universal mobile telecommunications system (UMTS) comprising at least two radio access networks providing mobile stations with access to at least one core network, a multimode mobile station, and at least one core network. During connection setup with a first radio access network, the mul-timode mobile station sends an unprotected initial signaling message that includes information about those encryption algorithms that the multimode mobile station supports when it communicates in a second radio access network. The first radio access network saves some or all the information of it. Then it composes and sends an integrity-protected message that includes information about the encryption algorithms supported by the multimode mobile station in the second radio access network.

WO 02/45453 A1

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

with international search report
with amended claims and statement

A SYSTEM FOR ENSURING ENCRYPTED COMMUNICATION AFTER HANDOVER

FIELD OF THE INVENTION

The present invention relates generally to an integrity protection in a telecommunications network.

BACKGROUND OF THE INVENTION

A third generation mobile communications system is in Europe named UMTS (Universal Mobile Telecommunications System). It is a part of the International Telecommunications Union's IMT-2000 system. UMTS/IMT-2000 is global wireless multimedia system which provides higher transmission speed (2 Mbit/s) than the existing mobile networks.

FIG. **1** shows with a simplified block diagram a GSM (Global System for Mobile communications) network and a UMTS network. The main parts of the network are user terminals **100** and a network part that comprises the GSM base station subsystem BSS **105** and the UMTS terrestrial radio access network UTRAN **101** (which is a wideband multiple access radio network currently being specified in the 3GPP (Third Generation Partnership Project)) and a core network CN **104**. The radio interface between a user terminal and the UTRAN is called Uu and the interface between the UTRAN and the 3G core network is called *Iu*. The interface between the GSM base station subsystem BSS and general packet radio service GPRS core network is called Gb and interface between the GSM base station subsystem BSS and GSM core networks is called A. The user terminals can be multi-mode terminals, which can operate using at least two radio access technologies, in this example UMTS and GSM. The UTRAN consists of a radio network subsystems RNS **102** that further consists of radio network controller RNC **103** and one or more nodes B (not shown in FIG.1). An interface between two RNS is called Iur. The interface between the user terminal and the GSM base station subsystem BSS is simply called "Radio Interface". The GSM base station subsystem BSS consists of the base station controllers BSC **106** and the base transceiver stations BTS **107**. The core network nodes, e.g. the (GSM) Mobile Switching Center MSC and the (GPRS) serving GPRS support node SGSN, can be capable of controlling both types of radio access networks - UTRAN and BSS. Another possible network configuration is such

that each radio access network (UTRAN and BSS) has its own controlling core network node, MSC and SGSN, respectively - 2G MSC, 2G SGSN and 3G MSC, 3G SGSN - but all these core network elements are connected to one and the same home location register HLR (not shown in FIG.1), which contains all static user information, e.g. the billing of users can be controlled from one location even when the user terminals are able to operate via several different radio access networks.

The radio interface protocols which are needed to set up, reconfigure and release the radio bearer services are discussed shortly in the following. The radio interface protocol architecture in the access stratum consists of three different protocol layers which are from top to bottom: the radio network layer (L3), the data link layer (L2), and the physical layer (L1). The protocol entities in these layers are the following. The radio network layer consists of only one protocol, which in the UMTS radio interface is called RRC (Radio Recourse Control) and in the 2G GSM radio interface is called RR (Radio Resource protocol). The data link layer consists of several protocols in the UMTS radio interface called PDCP (Packet Data Convergence Protocol), BMC (Broadcast Multicast Control protocol), RLC (Radio Link Control protocol), and MAC (Medium Access Control protocol). In the GSM/GPRS radio interface, the layer 2 protocols are LLC (Logical Link Control), LAPDm (Link Access Protocol on the Dm channel), RLC (Radio Link Control), and MAC (Medium Access Control protocol). The physical layer is only one 'protocol', which has no specific name. All the mentioned radio interface protocols are specific for each radio access technique, which means that they are different for the GSM radio interface and the UMTS Uu interface, for example.

In the UMTS, the RRC layer offers services to higher layers i.e. to a non access stratum NAS via service access points which are used by the higher protocols in the user terminal side and by the Iu RANAP (Radio Access Network Application Part) protocol in the UTRAN side. All higher layer signaling (mobility management, call control, session management, etc.) is encapsulated into RRC messages for transmission over the radio interface.

All telecommunication is subject to the problem of how to make sure that the information received has been sent by an authorized sender and not by somebody who is trying to masquerade as the sender. The problem is particularly evident in cellular telecommunication systems, where the

air interface presents an excellent platform for eavesdropping and replacing the contents of a transmission by using higher transmission levels, even from a distance. A basic solution to this problem is the authentication of the communicating parties. An authentication process aims to discover and check the identity of both the communicating parties, so that each party receives information about the identity of the other party and can rely on the identification to a sufficient degree. Authentication is typically performed in a specific procedure at the beginning of the connection. However, this does not adequately protect subsequent messages from unauthorized manipulation, insertion, and deletion. Thus, there is a need for the separate authentication of each transmitted message. The latter task can be carried out by appending a message authentication code (MAC-I) to the message at the transmitting end and checking the MAC-I value at the receiving end.

A MAC-I is typically a relatively short string of bits based in some specified way on the message it protects and on a secret key known both by the sender and by the recipient of the message. The secret key is generated and agreed on typically in connection with the authentication procedure at the beginning of the connection. In some cases the algorithm that is used to calculate the MAC-I based on the secret key and on the message is also secret, but this is not usually the case.

The process of authentication of single messages is often called integrity protection. To protect the integrity of signaling, the transmitting party computes a MAC-I value based on the message to be sent and the secret key using the specified algorithm, and sends the message with the MAC-I value. The receiving party recomputes a MAC-I value based on the message and the secret key according to the specified algorithm, and compares the received MAC-I and the calculated MAC-I. If the two MAC-I values match, the recipient can trust that the message is intact and has been sent by the authorized party.

FIG. **2** illustrates the computation of a message authentication code in the UTRAN. The length of the MAC-I used in UTRAN is 32 bits.

The UMTS integrity algorithm used in block **200** is a one-way cryptographic function for calculating the Message Authentication Code (MAC-I) based on the input parameters shown in FIG **2**. The one-way function means that it is impossible to derive the unknown input parameters from a MAC-I, even if all but one input parameter are known.

The input parameters for calculating the MAC-I are the actual signaling message (after encoding) to be sent, a secret integrity key, a sequence number COUNT-I for the message to be integrity protected, a value indicating the direction of transmission, i.e. whether the message is sent in uplink (from the user terminal to the network) or downlink (from the network to the user terminal) direction, and a random number (FRESH) generated by the network. COUNT-I is composed of a short sequence number SN and a long sequence number called hyper frame number HFN. Only the short sequence number is normally sent with the message; the HFN is updated locally at each communicating party.

The computing block **200** calculates the message authentication code by applying the afore-mentioned parameters to the integrity algorithm, which is called f9 algorithm in 3GPP Release'99 specifications. It is possible that more algorithms will be available in future releases of new specifications. Before integrity protection is started, the user terminal informs the network, which integrity algorithms it supports, and the network then selects one of these algorithms to be used for the connection. A similar mechanism regarding the supported algorithms is also used for the ciphering.

FIG. **3** illustrates a message to be sent over e.g. a radio interface. The message is a layer N protocol data unit (PDU) **300,** which is transferred as a payload in layer N-1 PDU **301**. In the present example, layer N represents the Radio Resource Control (RRC) protocol in the radio interface and layer N-1 represents the Radio Link Control (RLC) layer. The layer N-1 PDU normally has a fixed size, which depends on the physical layer (the lowest layer, not visible in FIG 2) channel type used and on the parameters, e.g. modulation, channel coding, interleaving. If layer N PDUs are not exactly the size of the payload offered by layer N-1 as is normally the case, layer N-1 can utilize functions like segmentation, concatenation, and padding to make layer N-1 PDUs always a fixed size. In the present application we are concentrating on a layer N PDU consisting of the actual signaling data and the Integrity Check Info. The Integrity Check Info consists of the MAC-I and the message sequence number SN needed at the peer end for the recalculation of MAC-I. The total length of the message is then a combination of the signaling data bits and the Integrity Check Info bits.

FIG. **4** illustrates intersystem handover from a radio access network to a GSM base station subsystem. For simplicity only one mobile

switching center is shown in the FIG. **4**. Actually it consists of a GSM (2G or second generation) mobile switching center MSC and a UMTS (3G or third generation) mobile switching center, which may be physically either one or two separate MSC's. Interaction between these two mobile switching centers (if they would be two separate entities) is not essential in view of the actual invention and therefore it is not described in the following.

At the beginning, a connection exists between the user terminal and the radio access network, which in this particular example is a UTRAN. Based on various parameters, e.g. the neighboring cell load information, measurements from the user terminal, and the existence of GSM cells in the nearby geographical area as well as existence of the user terminal capabilities (to support also GSM mode), the radio access network may initiate an intersystem handover to base station subsystem BSS. First, the UTRAN requests the user terminal to start intersystem measurements on GSM carriers by sending a MEASUREMENT CONTROL message **400** containing intersystem specific parameters. When the criteria (as described in the MEASUREMENT CONTROL message) to send a measurement report is fulfilled, the user terminal sends a MEASUREMENT REPORT(s) **401**. Intersystem handover decision is then made at the UTRAN. After the decision a serving radio network controller SRNC, which is located in the UTRAN, sends a RELOCATION REQUIRED **402** message through Iu interface to the mobile switching center (3G MSC). Once after receiving, the message the mobile switching center (2G MSC) sends a HANDOVER REQUEST message **403** to a target base station subsystem, containing information, such as the ciphering algorithm and ciphering key to be used for the connection, and the MS classmark information, indicating, for example, which ciphering algorithms are supported by the user terminal. Thus, it is possible that either the mobile switching center MSC selects the ciphering algorithm and indicates only the selected algorithm to the base station subsystem BSS, or that the mobile switching center MSC sends a list of possible ciphering algorithms to the base station subsystem BSS, which then makes the final selection. The MS classmark information was sent by the user terminal to the mobile switching center MSC at the beginning of the (UMTS) connection. It is also possible that the MS classmark information is sent from the user terminal to the UMTS radio access network (UTRAN) at the beginning of the (UMTS) connection. When an inter-system handover from UMTS to GSM is triggered, the MS

classmark information is forwarded from UTRAN to MSC. When a GSM base station controller receives the message it makes reservation from the indicated GSM cell and responds by sending back a HANDOVER REQUEST ACK message **404** indicating that the requested handover at the base station subsystem BSS can be supported and also to which radio channel(s) the user terminal should be directed. The HANDOVER REQUEST ACK **404** also indicates that the requested handover algorithm has been accepted, or, if the HANDOVER REQUEST **403** contained several algorithms, which handover algorithm has been selected. If the base station subsystem BSS is not able to support any of the indicated ciphering algorithms, it returns a HANDOVER FAILURE message (instead of **404**) and the mobile switching center MSC indicates failure of the handover to the UTRAN. At stage **405**, the mobile switching center (3G MSC) responds with a RELOCATION COMMAND message over the Iu interface to the message sent at stage **402** from the serving radio network controller located in the UTRAN. The RELOCATION COMMAND carries in a payload e.g. the information about the target GSM channels together with the cipher mode information. The UTRAN commands the user terminal to execute the handover by sending an INTERSYSTEM HANDOVER COMMAND **406** message including channel information for the target GSM. In addition, other information may be included, such as the GSM cipher mode setting information, which indicates at least the ciphering algorithm to be used in the GSM connection. After having switched to the assigned GSM channels, the mobile station normally sends four times the HANDOVER ACCESS message **407** in four successive layer 1 frames on the main DCCH. These messages are sent in GSM access bursts, which are not ciphered. In some situations it may not be necessary to send these HANDOVER ACCESS messages, if so indicated in the INTERSYSTEM HANDOVER COMMAND **406**. The terminal may receive a PHYSICAL INFORMATION **408** message as a response to the HANDOVER ACCESS messages. The PHYSICAL INFORMATION message contains only the GSM Timing Advance information. Reception of a PHYSICAL INFORMATION message causes the terminal to stop sending access bursts. The HANDOVER ACCESS messages, if used, trigger the GSM base station controller in the base station system to inform about the situation to the mobile switching center (2G) with a HANDOVER DETECT message **409.**

After lower layer connections are successfully established, the mobile station returns a HANDOVER COMPLETE **410** message to the GSM base station subsystem on the main DCCH. When receiving the HANDOVER COMPLETE message **410**, the network releases the old channels, in this example the UTRAN channels. In FIG. **4**, three messages from this release procedure are shown, although in reality many other messages between network elements, which are not shown in FIG. **4**, would be needed. These three messages are first the HANDOVER COMPLETE message **411** from GSM base station subsystem to the mobile switching center, then a IU RELEASE COMMAND **412** through Iu interface to the UTRAN or more accurately to the serving radio network controller. The third message is the IU RELEASE COMPLETE message **413**.

The ciphering key to be used after the intersystem handover is derived with a conversion function from the ciphering key used in UTRAN before the handover. This conversion function exists both in the mobile station and in the mobile switching center, thus no extra procedures over the radio interface are needed. As described above, the GSM ciphering algorithm to be used after the intersystem handover is selected either by the MSC or by the BSS and informed to the mobile station (in messages **405** and **406**). The GSM Ciphering algorithm capability (included in the GSM MS classmark information elements) is in current specifications transparent to the UTRAN. However, the GSM MS classmark information elements are sent from the mobile station to UTRAN during the RRC Connection Establishment procedure, to be later forwarded to the core network during the inter-system handover to GSM.

FIG. **5** is a signaling diagram showing the basic connection setup and security mode setup procedure used in the 3GPP UTRAN. FIG. **5** shows only the most important signaling between a mobile station and a serving radio network controller residing in the radio access network on the one hand and the serving radio network controller and a mobile switching center or a serving GPRS support node on the other.

Establishment of a radio resource control (RRC) connection between the mobile station and the serving radio network controller is performed through Uu interface **500**. During RRC connection establishment, the mobile station may transfer information such as the user equipment security capability and the START values, which are required for the ciphering and

integrity protection algorithms. The user equipment security capability includes information about the supported (UMTS) ciphering algorithms and (UMTS) integrity algorithms. All the values mentioned above are stored for later use in the serving radio network controller at stage **501**. Also the GSM Classmark information (MS Classmark 2 and MS Classmark 3) is transmitted from the mobile station to UTRAN during RRC connection establishment, and it can be stored for later use in the serving radio network controller.

Next the mobile station sends an initial higher layer message **502** (which can be e.g. CM SERVICE REQUEST, LOCATION UPDATING REQUEST or CM RE-ESTABLISHMENT REQUEST) via the serving radio network controller through a *Iu* interface to the mobile switching center, including e.g. the user identity, a key set identifier KSI and the MS classmark indicating, for example, the supported GSM ciphering algorithms whenf intersystem handover to the GSM is initialized. The network initiates authentication procedure which also leads to generation of new security keys **503.** Next, the network decides the set of UMTS Integrity Algorithms UIAs and UMTS Encryption Algorithms UEAs from which the UIA and UEA for this connection has to be selected **504**. Then, at stage **505**, the mobile switching center sends a SECURITY MODE COMMAND message to the serving radio network controller, in which it informs the used ciphering key CK, integrity key IK, and the set of permissible UIAs and UEAs.

On the basis of the user equipment security capabilities stored at stage **501** and the list of possible UIAs and UEAs received from the mobile switching center at stage **505**, the serving radio network controller selects the algorithms to be used during the connection. It also generates a random value FRESH to be used as input parameter for the integrity algorithm (Fig. 2) and for the ciphering algorithm. It also starts deciphering and the integrity protection **506**.

A first integrity protected message SECURITY MODE COMMAND **507** is sent through the radio interface from the serving radio network controller to the mobile station. The message includes the selected UIA and UEA together with the UE FRESH parameter to be used. In addition, the SECURITY MODE COMMAND contains the same UE security capability which was received from the user equipment during the RRC connection establishment **500**. The reason for replaying this information back to UE is to give the user equipment a possibility to check that the network has received this informa-

tion correctly. This mechanism is necessary, since the messages sent during RRC connection establishment **500** are not ciphered nor integrity protected. A message authentication code MAC-I, used for the integrity protection, is attached to the SECURITY MODE COMMAND message **507**.

At stage **508** the mobile station compares whether the received UE security capability is same as that which has been sent during the RRC connection establishment procedure **500.** If the two UE security capabilities match, the mobile station can trust that the network has received the security capability correctly. Otherwise, the UE releases the RRC connection and enters idle mode.

If comparison is successful the mobile station responds with a SECURITY MODE COMPLETE message **509.** This is also an integrity protected message; thus before sending this message the mobile station generates the MAC-I for the message.

When the serving radio network controller receives the message it verifies it, at stage **510,** first by calculating the expected message authentication code XMAC-I and then comparing the calculated XMAC-I with the received MAC-I. If the values match, the serving radio network controller sends a SECURITY MODE COMPLETE message **511** to the mobile switching center including e.g. information of the selected UIA and UEA.

In the UTRAN radio interface integrity protection is a function of the radio recourse control protocol between the user terminal and the radio network controller. All higher layer signaling is integrity protected by the radio resource control protocol layer because all higher layer signaling is carried as a payload in specific radio recourse control messages (e.g. INITIAL DIRECT TRANSFER, UPLINK DIRECT TRANSFER, DOWNLINK DIRECT TRANSFER). The problem is that no authentication can be performed before the first higher layer message is sent, which is carried in the INITIAL DIRECT TRANSFER. This leads to a situation where the very first higher layer i.e. the non-access stratum message **502** cannot be integrity protected.

A major problem arises from the fact that integrity protection is not yet in effect when the first messages are sent during RRC Connection Establishment (step **500** in the FIG. **5**). Without integrity protection there is always a risk that an intruder changes the encryption algorithm information included in the messages at step **500** into the value "GSM encryption algorithms not available". In the case of GSM, the core network receives this information

with the mobile station classmark CM information elements (CM2 and CM3) that are included in the RELOCATION REQUIRED message (message **402** in FIG. **4**). When the user equipment carries out an intersystem handover, e.g. from the UTRAN to the GSM base station subsystem BSS (FIG. **4**) the mobile switching center recognizes that the UE does not support any GSM ciphering algorithms and must set up the connection in the GSM BSS with no ciphering. Now it is easy to the intruder to start eavesdropping of the call.

SUMMARY OF THE INVENTION

An objective of the present invention is to devise a mobile telecommunications system that reveals an attempt of a fraudulent intruder to remove information about an encryption algorithm when a multimode mobile station sends an unprotected signaling message containing this information over radio interface to the mobile telecommunications system. According to existing specifications, this signaling message is RRC CONNECTION SETUP COMPLETE.

The system comprises at least two radio access networks providing mobile stations with access to at least one core network, a multimode mobile station, and at least one core network. The multimode mobile station sends, during connection setup with a first radio access network, at least one unprotected signaling message, including information about encryption algorithms supported by the multimode mobile station in a second radio access network. The core network receives information about the encryption algorithms via the first radio access network when a handover to the second radio access network is triggered (message **402** in FIG **4**). The first radio access network has inventive features. Namely, in receipt of a command message from the core network instructing the multimode mobile station to cipher further communication in the first radio access network, the first radio access network composes an integrity protected command message that includes information about the encryption algorithms supported by the multimode mobile station in the second radio access network.

The protected command message comprises a payload and a message authentication code. The information about the supported algorithms in the second radio access network is located either in the payload or the information is used as a parameter when computing the message authentication code.

In both cases the multimode mobile station is able to conclude from the protected message received whether the information embedded in the message corresponds to the information sent by the multimode mobile station in the previous signaling message. If the information sent and the information received by the multimode mobile station differ from each other, it is likely that a fraudulent intruder has changed the encryption information. Then the multimode mobile station initiates release of the connection.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described more closely with reference to the accompanying drawings, in which

- FIG. **1** illustrates with a simplified block diagram a GSM and a UMTS radio access networks, connected to the same core network;
- FIG. **2** depicts the computation of a message authentication code;
- FIG. **3** shows the contents of a message;
- FIG. **4** is a signaling chart illustrating intersystem handover from the UMTS network to the GSM network;
- FIG. **5** is a signaling chart showing the basic connection setup and security mode setup procedure used in the 3GPP UTRAN;
- FIG. **6** shows as a flowchart of the first example of the implementation of the method according to the invention;
- FIG. **7** shows as a flowchart of a second example of the implementation of the method according to the invention;
- FIG. **8** shows as a flowchart of a third example of the implementation of the method according to the invention;
- FIG. **9** shows as a flowchart of a fourth example of the implementation of the method according to the invention;
- FIG. **10** shows a fifth example of the implementation of the method according to the invention;
- FIG. **11** shows a sixth example of the implementation of the method according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The idea of the method described in the following is to increase security in telecommunications network, especially security pertaining to signaling through the radio interface.

It is to be noted that all the terms "terminal", "user terminal", "mobile station" and "user equipment" refer to the same equipment.

Most signaling messages sent between a user terminal and the network, for example, must be integrity protected. Examples of such messages are RRC, MM, CC, GMM and SM messages. Integrity protection is applied at the RRC layer, both in the user terminal and in the network.

Integrity protection is usually performed for all RRC (Radio Recourse Control) messages, with some exceptions. These exceptions can be:

1. messages assigned to more than one recipient,
2. messages sent before the integrity keys were created for the connection, and
3. frequently repeated messages, including information not needing integrity protection.

Due to security, it is especially important to integrity protect the initial messages mentioned in alternative 2, or at least critical information elements in them. As already mentioned, without integrity protection there is always a risk that an intruder changes the encryption algorithm information included into message **500** to the value "encryption algorithm is not available".

There are several different ways of implementing the functionality required to increase security but only some of solutions are shown.

The invention is now described in detail with four examples by referring to FIG. **6** –**9**.

In the beginning a connection is established between a user terminal and a UMTS network. Afterwards a handover is carried out from the UMTS network to a GSM network.

FIG. **6** shows as a flowchart of one implementation of the method according to the invention. It is assumed that signaling corresponds to the situation shown in FIG. **5** until the core network receives message **503**.

In addition it is assumed that the user terminal is a dual mode (UMTS/GSM) terminal, which on the UMTS mode sends the first non-access-stratum message over the radio interface in a radio resource control INITIAL

DIRECT TRANSFER message (corresponding message **502** in FIG. **5**). It is further assumed that the RRC Connection Establishment (500) has been performed, thus the user terminal was in an idle state and had no existing RRC Connection when a request arrived to set up a connection with the core network.

The core network receives GSM classmark information in the initial message **502** from the user terminal, here the mobile station. This information indicates general mobile station characteristics in the GSM mode including information about which GSM ciphering algorithms are supported at the terminal when it is in GSM mode. The term "classmark" has to be understood as GSM specific; another term may be used in other systems. The mobile switching center in the core network adds information about encryption algorithms supported by the mobile station into the SECURITY MODE COMMAND message **600**. The message is sent to the serving radio network controller through the *Iu* interface. The serving radio network controller adds this information about encryption algorithms supported by the mobile station, including information about supported encryption algorithms, to a SECURITY COMMAND message before encoding **601**. A 32-bit message authentication code MAC-I is computed and added to the encoded message.

Besides the encoded message the MAC-I code is also based on several other parameters. The following input parameters are needed for computation of the integrity algorithm: the encoded message, the 4-bit sequence number SN, the 28-bit hyper-frame number HFN, the 32-bit random number FRESH, the 1-bit direction identifier DIR, and the most important parameter - the128-bit integrity key IK. The short sequence number SN and the long sequence number HFN together compose the serial integrity sequence number COUNT-I.

When the message authentication code is computed using the integrity algorithm and the above parameters, it is guaranteed that no one other than the actual sender can add the correct MAC-I code to the signaling message. COUNT-I, for example, prevents the same message from being sent repeatedly. However, if the same signaling message for some reason or other is to be sent repeatedly, the MAC-I code differs from the MAC-I code that was in the previously sent signaling message. The aim of this is to protect the message as strongly as possible against eavesdroppers and other fraudulent users. Thus, for this particular invention, it is important to note that

also the GSM information about encryption algorithms supported by the mobile station is added to the SECURITY MODE COMMAND message 507, is integrity protected, so that the mobile station can be sure that this information has not been changed by an intruder.

Next, at stage **602**, when the mobile station receives the SECURITY MODE COMMAND message, the information about encryption algorithms supported by the mobile station received with this message is compared with the information about encryption algorithms supported by the mobile station sent earlier from the mobile station to the network in the initial message **502**. Correspondingly, according to prior art, the received UE (UMTS) security capability parameter is compared with the sent UE security capability parameter. If both comparisons are successful the mobile station accepts the connection **604**, otherwise the connection is released **603**.

FIG. **7** shows as a flowchart of the second implementation of the method.

At stage **700** the mobile station sends an INITIAL DIRECT TRANSFER message (corresponding to message **502** in FIG. **5**) to the core network via the serving radio network controller in the radio access network. The message consists of two main parts: a RRC part and a non-access stratum part, which is seen by the RRC as a transparent payload. Moreover, the payload part includes one of the following messages: CM SERVICE REQUEST, LOCATION UPDATING REQUEST, CM RE-ESTABLISHMENT REQUEST or PAGING RESPONSE.

When the serving radio network controller receives the message it stores the message **701** and forwards the payload part or the NAS part through the Iu interface to the core network **702**. The core network responds with the normal SECURITY MODE COMMAND message **703**. As in the previous example, the message authentication code MAC-I is computed to protect the message to be transmitted to the mobile station. The code is then added to the message. The message authentication code depends in a specified way on the message that it is protecting. Here computation is carried out using the following concatenated bit string as a MESSAGE parameter:

MESSAGE = SECURITY MODE COMMAND + RRC CONNECTION REQUEST + RRC INITIAL DIRECT TRANSFER.

Thereafter, the integrity protected SECURITY MODE COMMAND message is sent to the mobile station **704**.

It should be noted that in this solution it is unnecessary to include the UE (UMTS) security capability parameter into the above message. However, both security related parameters, i.e. the UE security capability parameter and the GSM classmark parameter were input parameters when the MAC-I code was computed.

The receiving end, i.e. the mobile station, has the identical algorithm for computing the message authentication code in order to verify that the message authentication code received is the same as the computed code **705**. Thus, the mobile station has saved the messages earlier sent, the RRC CONNECTION REQUEST message (**500**) and the RRC INITIAL DIRECT TRANSFER message (**502**) in order to calculate XMAC-I for the received SECURITY MODE COMMAND message. When the MAC-I value received and the computed XMAC-I value match, the mobile station assumes that the network has received correct information as to the security capability and the GSM classmarks, and the connection is accepted **707.** Otherwise the connection is released **706**.

There is one drawback of this solution, which is that the encoded messages RRC CONNECTION REQUEST and RRC INITIAL DIRECT TRANSFER must be stored in the memory of both the serving radio network controller and the mobile station until the SECURITY MODE COMMAND message has been sent/received. But on the other hand, this solution makes it possible to omit the UE security capability from the prior art SECURITY MODE COMMAND message and in this way to save 32 bits space in the message.

FIG. **8** shows as a flowchart of the third implementation of the method.

This solution differs slightly from the second solution, i.e. only blocks **801, 804** and **805** differ from the blocks in FIG. **7**. Therefore, these two blocks are now described in detail.

At stage **801,** instead of storing the whole message the serving radio network controller stores only the payload part of the message for later use. In other words, it stores one of the following messages: CM SERVICE REQUEST, LOCATION UPDATING REQUEST, CM RE-ESTABLISHMENT

REQUEST or PAGING REQUEST. Thus, this solution saves memory space as compared to the second solution.

At stage **804**, to protect the message the message authentication code MAC-I is computed by using the previously stored payload. The MESSAGE is formed in this case as follows:

MESSAGE = SECURITY MODE COMMAND + UE SECURITY CAPABILITY + NAS message part of the INITIAL DIRECT TRANSFER message.

Only the SECURITY MODE COMMAND message is sent over the Uu interface to the mobile station. This means that both the security parameters for the UE security capability and the GSM MS classmarks are used in computing the message authentication code MAC-I, but there is no need to include them in the message. However, this does not in any way decrease the security.

At stage **805** the mobile station computes the XMAC-I by using the same MESSAGE parameter as the network used at stage **804**, i.e. the parameters, which were saved earlier of the UE Security Capability and the NAS message part of the INITIAL DIRECT TRANSFER message.

FIG. **9** shows as a flowchart the fourth implementation of the method. This solution is a combination of the first and the third solutions.

During connection establishment between the mobile station and the serving radio network controller in the radio access network, the latter receives and stores the user equipment capability information UEC in its memory for later use **900**. After that the mobile station sends the first non-access stratum message containing e.g. information about encryption algorithms supported by the mobile station, as a payload in a RRC INITIAL DIRECT TRANSFER message to the radio access network, which forwards the NAS message to the core network **901**. The mobile switching center in the core network adds the information about encryption algorithms supported by the mobile station parameter to the SECURITY MODE COMMAND message and sends the message through the *Iu* interface to the serving radio network controller in the radio access network, at stage **902** and **903**.

At stage **904** the serving radio network controller computes the MAC-I code in the previously described way, adding to the earlier described parameters the MESSAGE parameter, which is formed as follows:

MESSAGE = SECURITY MODE COMMAND + UE SECURITY CAPABILITY + GSM CLASSMARKS.

In the same way as in the previous example, both the security parameters UE security capability and the GSM classmark are used for computing the message authentication code MAC-I, but there is no need to include them in the message. The advantage of this solution is that no additional memory is needed in the mobile station or in the radio network controller.

It is essential that in the solutions described above the core network is a 3G network element, thus controlling at least UMTS Radio Access Network and optionally also the GSM Base Station Subsystem.

Implementation and embodiment of the present invention has been explained above with some examples. However, it is to be understood that the invention is not restricted to the details of the above embodiment and that numerous changes and modifications can be made by those skilled in the art without departing from the characteristic features of the invention. The embodiment described is to be considered illustrative but not restrictive. Therefore, the invention should be limited only by the attached claims. Thus, alternative implementations defined by the claims, as well as equivalent implementations, are included in the scope of the invention.

For example, the source radio access network can be, for example, the UTRAN, the GSM base station subsystem, the GPRS system (General Packet Radio Service), the GSM Edge, the GSM 1800, or some other system. Correspondingly, the target radio access network can be, for example, the UTRAN, the GSM base station subsystem, the GPRS (General Packet Radio Service), the GSM Edge, the GSM 1800, or some other system.

Furthermore, information about GSM security algorithms (A5/1, A5/2, A5/3, etc.) that are supported by the multi-mode mobile terminal can be added as a part of the UMTS "UE Radio Access Capability". Alternatively, the information can be a separate information element or even a part of the UE security capability parameter. In practice this information must be added to the RRC connection establishment procedure (see stage **500** in FIG. **5**), as well as to the SECURITY MODE COMMAND message (see stage **507** in FIG.**5**). Like in the other possible implementations described earlier, also in this case adding the actual "Inter-RAT Radio Access Capability" (including information about supported GSM security algorithms) information element to

the RRC SECURITY MODE COMMAND message is just one alternative and introduces some overhead to the signaling, since the mobile does not necessarily need this information element, but only a confirmation that the network has received it correctly. Three alternative solutions, i.e. the fifth, sixth, and seventh example implementations of the method are described in the following.

In the fifth example of the implementation of the method, a new RRC information element, including only the GSM ciphering algorithm capability, is defined. This requires 7 bits. This information element is then added to the RRC SECURITY MODE COMMAND message. The drawback of this solution is that to encode this new information element into the said message, UTRAN RRC protocol first has to decode the GSM classmark 2 and classmark 3 information elements, whose encoding/decoding rules are not part of the UTRAN RRC protocol.

FIG. **10** illustrates the sixth example of the implementation of the method. On the UTRAN side, the GSM Classmark 2 and Classmark 3 information received (RRC information element "Inter-RAT UE radio access capability" **1001**), together with the "UE Security Capability" **1002** (containing information about supported UTRAN security algorithms), are used for calculating MAC-I (and XMAC-I) for the RRC SECURITY MODE COMMAND message **1000**. This is essentially the same solution as in FIG 9 with the exception that the GSM Classmark information (from the mobile station and not from the core network (902)) has already been received and stored in the serving radio network controller during the RRC Connection Establishment phase (900). The SECURITY MODE COMMAND to be sent to the mobile station does not contain "UE security capability" nor "Inter-RAT UE radio access capability"; these information elements are only used when calculating the MAC-I for this message.

The drawback of the sixth implementation is that the coding of the extra information elements ("UE security capability" and "Inter-RAT UE radio access capability") used for the MAC-I calculation has to be explicitly defined. If this is not acceptable, a more straightforward implementation is shown in FIG. **11** (a seventh implementation of the method). Here the entire encoded RRC_CONNECTION_SETUP_COMPLETE message is used when calculating MAC-I (and XMAC-I) for the RRC_SECURITY_MODE_COMMAND message **1000** (instead of the two information elements only as in the sixth im-

plementation). In practice this means that during the RRC connection establishment procedure (see stage **500** in FIG. **5**), when sending the RRC_CONNECTION_SETUP_COMPLETE message the mobile station must save a copy of the encoded message in its memory until it receives the SECURITY_MODE_COMMAND message and has checked its integrity checksum. On the network side (in the case of UTRAN in the serving radio network controller) a copy of the (non-decoded) RRC_CONNECTION_SETUP_COMPLETE message received must be kept in the memory until the MAC-I code for the SECURITY_MODE_COMMAND message has been calculated. From the standpoint of implementation, it is probably quite easy to save the entire encoded message in the memory before it is sent (UE side) or just after receiving it and before it is passed to the decoder (UTRAN side). Thus, MAC-I for SECURITY_MODE_COMMAND would be calculated by setting the MESSAGE-input parameter for the integrity algorithm as:

MESSAGE = SECURITY_MODE_COMMAND + RRC_CONNECTION_SETUP_COMPLETE

The drawback here, as compared to the sixth example of the implementation of the method, is that this solution requires a bit more memory, both in the mobile station and on the network side. The GSM classmark information includes the encryption algorithms supported by the mobile station.

Claims

1. A mobile telecommunications system comprising:

a plurality of radio access networks providing mobile stations with access to at least one core network;

a multimode mobile station sending, during connection setup with a first radio access network, at least one unprotected initial signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network;

a core network receiving information about the encryption algorithms,

the first radio access network being adapted to

receive a command message from the core network instructing the multimode mobile station to cipher further communication:

compose and send the multimode mobile station an integrity protected command message including information about the encryption algorithms supported by the multimode mobile station in the second radio access network, the protected command message comprising a payload and a message authentication code, and

the multimode mobile station being adapted to conclude whether the information about the encryption algorithms received in the integrity protected command message corresponds to the information sent by the multimode mobile station in the initial signaling messages.

2. A system as in claim 1, wherein the unprotected initial signaling message is sent, when performing handover from the core network comprising at least one mobile telecommunications switching element for packet-switched communication to the mobile telecommunications switching center for circuit-switched communication.

3. A system as in claim 1, wherein the first radio access network attaches information about the encryption algorithm received in the command message to the payload of the protected command message and applies the payload to an algorithm computing the message authentication code.

4. A system as in claim 1, wherein the first radio access network saves the unprotected initial signaling message received from the multimode mobile station and uses said message in computing the message authentication code.

5. A system as in claim 1, wherein the first radio access network saves the payload of the unprotected initial signaling message received from the multimode mobile station and uses said payload in computing the message authentication code.

6. A system as in claim 1, wherein the first radio access network saves information about mobile station's capability received from the mobile station during connection setup, and in computing the message authentication code uses said information together with information about the encryption algorithm embedded in the command message received from the core network.

7. A system as in claim 1 or 6, wherein the mobile station sends information about encryption algorithms during the connection setup, the first radio access network saves said information and uses said information in composing the protected command message.

8. A radio access network for providing multimode mobile stations with access to at least one core network,

the radio access network being adapted to

receive from a multimode mobile station via a radio interface an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in another radio access network, and forward the information to the core network,

receive a first command message from the core network instructing the multimode mobile station to cipher further communication;

compose a second command message comprising of a payload and a message authentication code,

compute the message authentication code by using as one of the computing parameters information about the encryption algorithms supported by the multimode mobile station in another network, and

send the second command message to the multimode mobile station.

9. A radio access network as in claim 8, wherein information about the encryption algorithms is attached to the payload of the second command message.

10. A radio access network as in claim 8, wherein the unprotected initial signaling message received from the multimode mobile station is saved and said message is used in computing the message authentication code.

11. A radio access network as in claim 8, wherein the payload of the unprotected initial signaling message received from the multimode mobile station is saved and the saved payload is used in computing the message authentication code.

12. A radio access network as in claim 8, wherein information about the encryption algorithm supported by the multimode mobile station is attached to a message sent during connection setup before the unprotected signaling message, said information being used in computing the message authentication code.

According to the Article 19 we use the opportunity to amend the claims of the above-identified international application.

Enclosed please find a Statement under Article 19(1) as well as replacement sheets 20 and 21 which substitute the sheets 20, 21 and 22 as filed.

The differences between the replaced sheets and the replacement sheets are explained in the Statement enclosed within this letter.

Claims

1. A mobile telecommunications system comprising:

a plurality of radio access networks providing mobile stations with access to at least one core network;

a multimode mobile station sending, during connection setup with a first radio access network, at least one unprotected initial signaling message including information about encryption algorithms supported by the multimode mobile station in a second radio access network;

a core network receiving information about the encryption algorithms,

the first radio access network being adapted to

receive a command message from the core network instructing the multimode mobile station to cipher further communication:

compose and send the multimode mobile station an integrity protected command message including information about the encryption algorithms supported by the multimode mobile station in the second radio access network, the protected command message comprising a payload including a message authentication code, and

the multimode mobile station being adapted to conclude whether the information about the encryption algorithms received in the integrity protected command message corresponds to the information sent by the multimode mobile station in the initial signaling messages.

2. A system as in claim 1, wherein the first radio access network attaches information about the encryption algorithm received in the command message to the payload of the protected command message and applies the payload to an algorithm computing the message authentication code.

3. A system as in claim 1, wherein the first radio access network saves the unprotected initial signaling message received from the multimode mobile station and uses said message in computing the message authentication code.

4. A system as in claim 1, wherein the first radio access network saves the payload of the unprotected initial signaling message received from the multimode mobile station and uses said payload in computing the message authentication code.

5. A system as in claim 1, wherein the first radio access network saves information about mobile station's capability received from the mobile station during connection setup, and in computing the message authentication code uses said information together with information about the encryption algorithm embedded in the command message received from the core network.

6. A system as in claim 1 or 5, wherein the mobile station sends information about encryption algorithms during the connection setup, the first radio access network saves said information and uses said information in composing the protected command message.

7. A radio access network for providing multimode mobile stations with access to at least one core network,

the radio access network being adapted to

receive from a multimode mobile station via a radio interface an unprotected signaling message including information about encryption algorithms supported by the multimode mobile station in another radio access network, and save this information for future use,

receive a first command message from the core network instructing the multimode mobile station to cipher further communication;

compose a second command message comprising of a payload including a message authentication code,

compute the message authentication code by using as one of the computing parameters information about the encryption algorithms supported by the multimode mobile station in another radio access network, and

send the second command message to the multimode mobile station.

8. A radio access network as in claim 7, wherein information about the encryption algorithms is attached to the payload of the second command message.

9. A radio access network as in claim 7, wherein the unprotected initial signaling message received from the multimode mobile station is saved and said message is used in computing the message authentication code.

10. A radio access network as in claim 7, wherein the payload of the unprotected initial signaling message received from the multimode mobile station is saved and the saved payload is used in computing the message authentication code.

STATEMENT UNDER ARTICLE 19(1)

Following amendments have been made to the claims to make the concept of the present invention clearer:

new claim 1 corresponds to the previous claim 1, but the word "and" in line 17 is removed and replaced by the word: "*including*",

previous claim 2 is deleted,

new claims 2-6 correspond the previous claims 3-7 with corrected references where appropriate,

new claim 7 corresponds the previous claim 8, but the following words in line 21: "forward the information to the core network" has been removed and replaced by the words: "*save this information for future use*",
the word "and" in line 25 is removed and replaced by the word: "*including*", and further
the words "in another network" in line 28 are replaced by the words: "in another *radio access* network",

new claims 8-10 correspond the previous claims 9-11 with corrected references where appropriate,

previous claim 12 is deleted.

The applicant respectfully confirms that no new matter has been incorporated into the amended claims. The amendments have no impact on the description and the drawings.

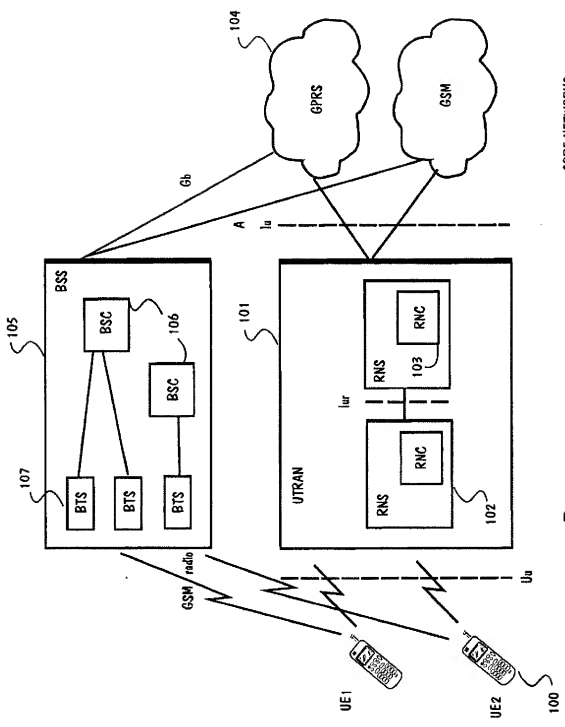
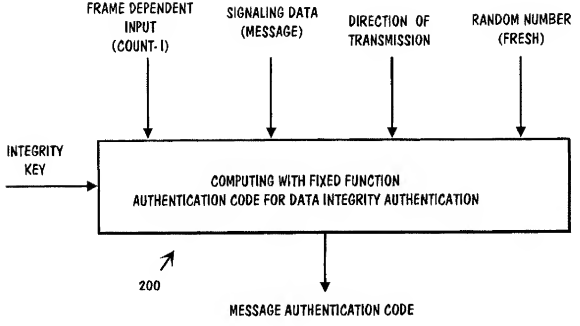
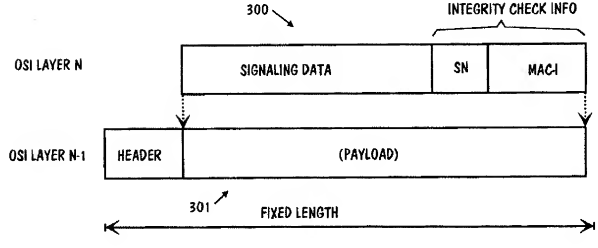


Fig. 1 PRIOR ART



PRIOR ART

Fig. 2



PRIOR ART

Fig. 3

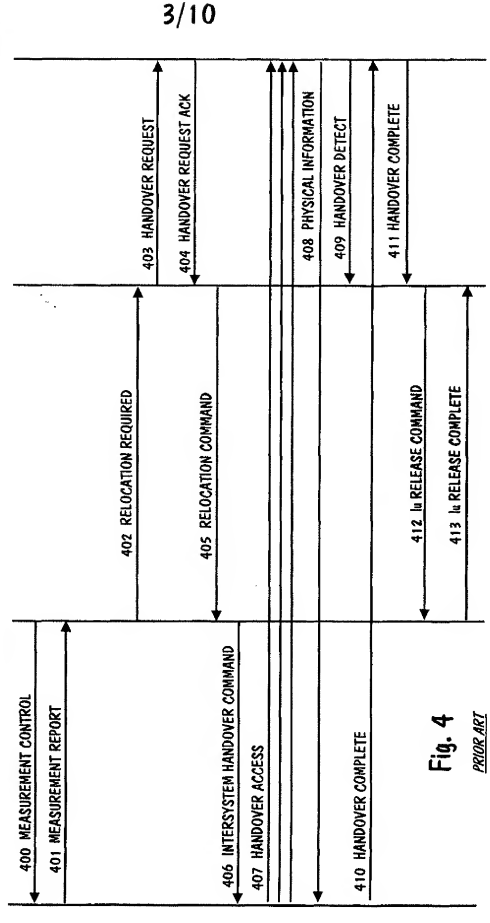


Fig. 4
PRIOR ART

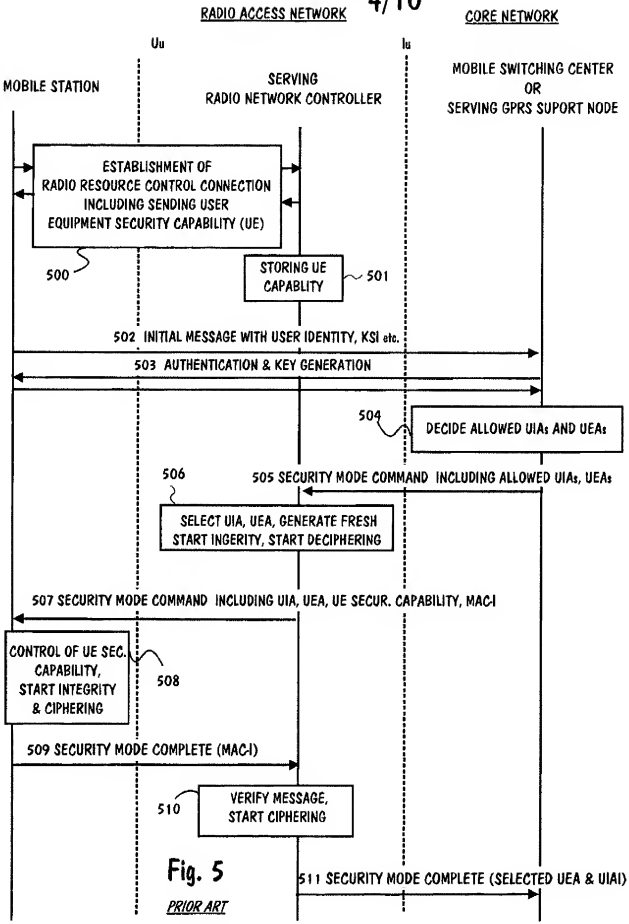
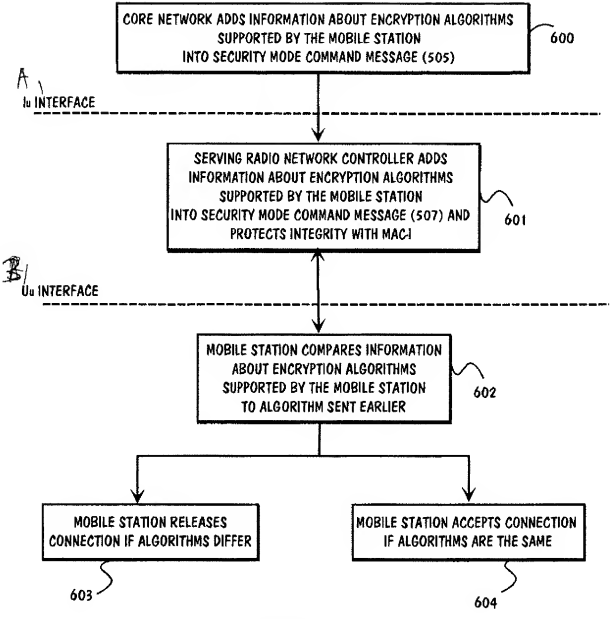


Fig. 5

PRIOR ART



SOLUTION 1

Fig. 6

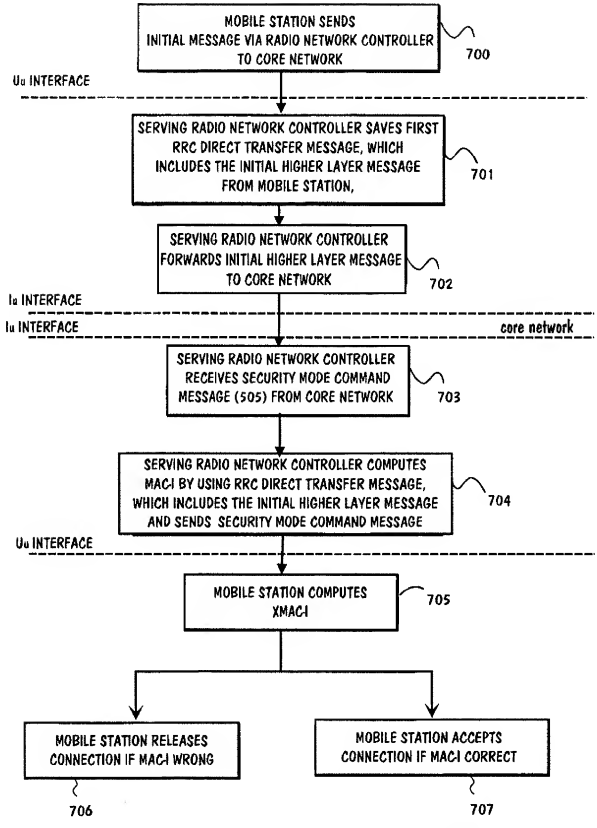
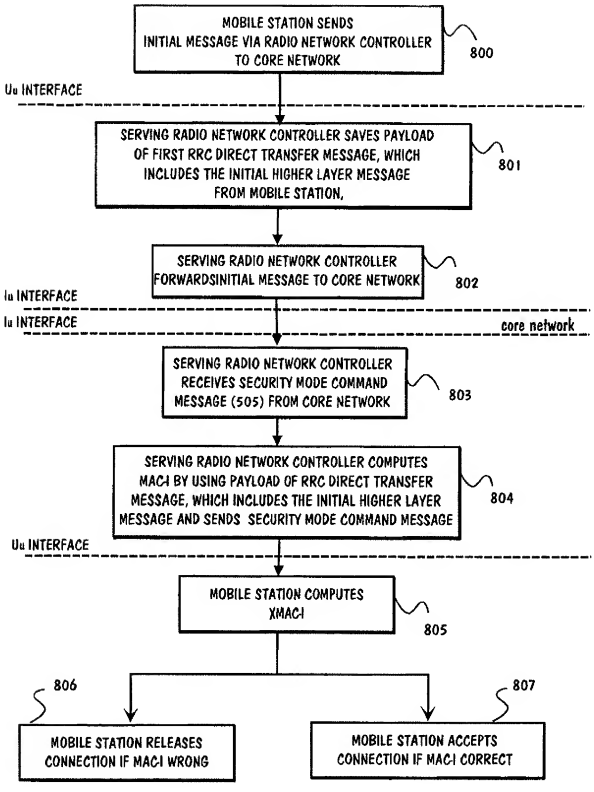


Fig. 7

SOLUTION 2



SOLUTION 3

Fig. 8

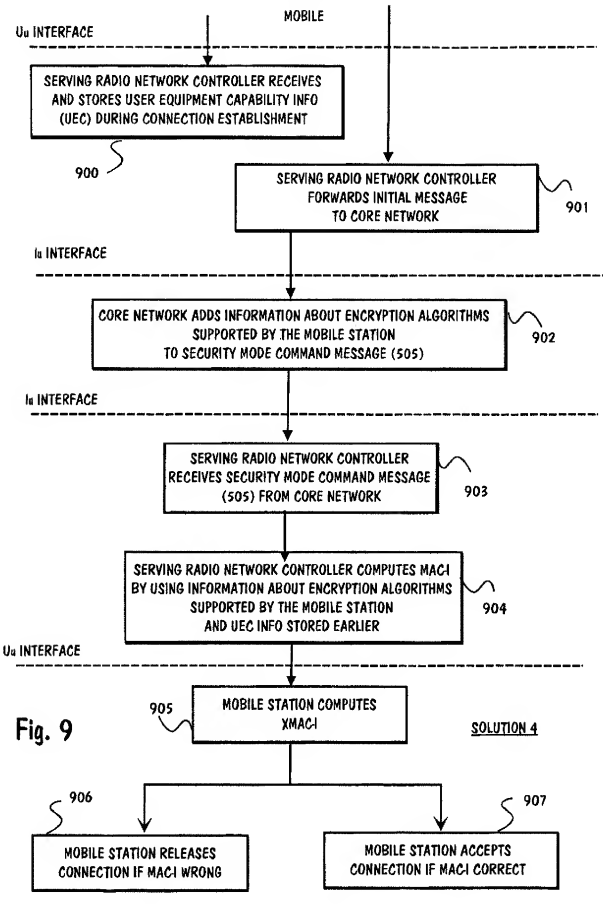

MOBILE
Uu INTERFACE
SERVING RADIO NETWORK CONTROLLER RECEIVES AND STORES USER EQUIPMENT CAPABILITY INFO (UEC) DURING CONNECTION ESTABLISHMENT
900
SERVING RADIO NETWORK CONTROLLER FORWARDS INITIAL MESSAGE TO CORE NETWORK
901
Iu INTERFACE
CORE NETWORK ADDS INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION TO SECURITY MODE COMMAND MESSAGE (505)
902
Iu INTERFACE
SERVING RADIO NETWORK CONTROLLER RECEIVES SECURITY MODE COMMAND MESSAGE (505) FROM CORE NETWORK
903
SERVING RADIO NETWORK CONTROLLER COMPUTES MAC-I BY USING INFORMATION ABOUT ENCRYPTION ALGORITHMS SUPPORTED BY THE MOBILE STATION AND UEC INFO STORED EARLIER
904
Uu INTERFACE
905
MOBILE STATION COMPUTES XMAC-I
SOLUTION 4
906
MOBILE STATION RELEASES CONNECTION IF MAC-I WRONG
907
MOBILE STATION ACCEPTS CONNECTION IF MAC-I CORRECT

Fig. 9

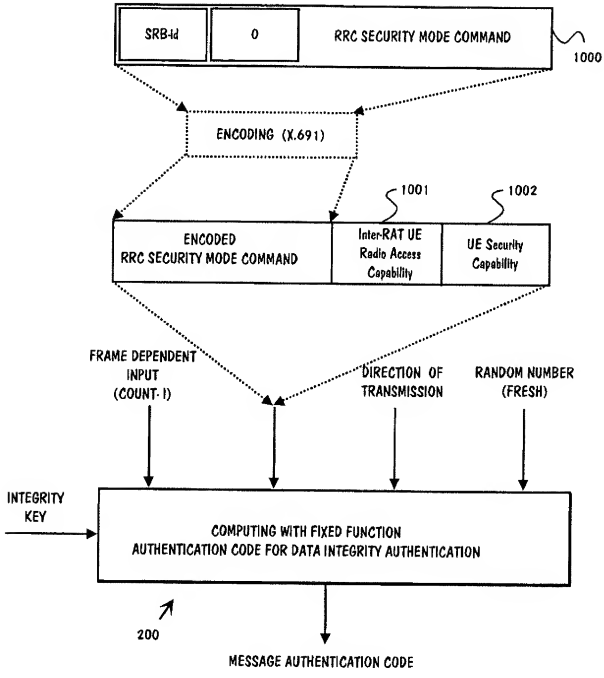

SRB-id
0
RRC SECURITY MODE COMMAND
1000
ENCODING (X.691)
1001
1002
ENCODED RRC SECURITY MODE COMMAND
Inter-RAT UE Radio Access Capability
UE Security Capability
FRAME DEPENDENT INPUT (COUNT-I)
DIRECTION OF TRANSMISSION
RANDOM NUMBER (FRESH)
INTEGRITY KEY
COMPUTING WITH FIXED FUNCTION AUTHENTICATION CODE FOR DATA INTEGRITY AUTHENTICATION
200
MESSAGE AUTHENTICATION CODE
SOLUTION 6

Fig. 10

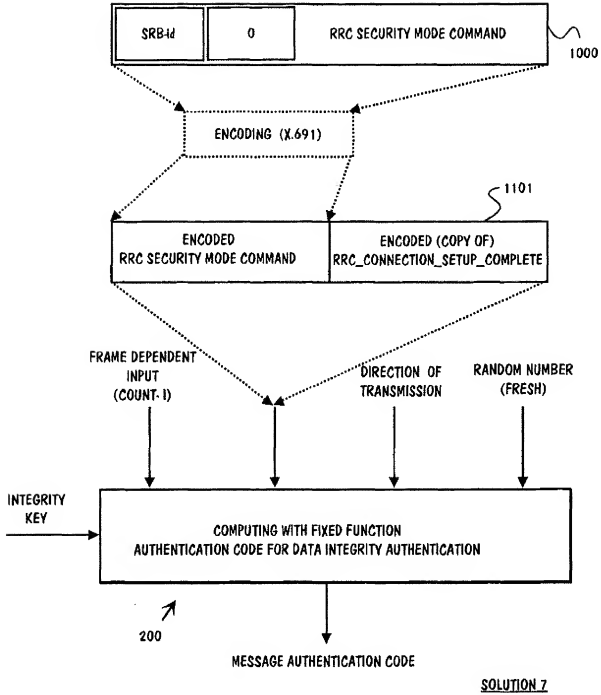

SRB-Id
0
RRC SECURITY MODE COMMAND
1000
ENCODING (X.691)
1101
ENCODED
RRC SECURITY MODE COMMAND
ENCODED (COPY OF)
RRC_CONNECTION_SETUP_COMPLETE
FRAME DEPENDENT
INPUT
(COUNT- I)
DIRECTION OF
TRANSMISSION
RANDOM NUMBER
(FRESH)
INTEGRITY
KEY
COMPUTING WITH FIXED FUNCTION
AUTHENTICATION CODE FOR DATA INTEGRITY AUTHENTICATION
200
MESSAGE AUTHENTICATION CODE
SOLUTION 7

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00870

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI DATA, EPO INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9926420 A2 (NOKIA TELECOMMUNICATIONS OY), 27 May 1999 (27.05.99), figures 1,2, abstract --	1-12
A	WO 9837721 A2 (NOKIA TELECOMMUNICATIONS OY), 27 August 1998 (27.08.98), figure 1, abstract --	1-12
P,A	EP 1111952 A2 (NOKIA CORPORATION), 27 June 2001 (27.06.01), abstract -- ---	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 February 2002	18 -02- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/02

International application No.
PCT/FI 01/00870

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9926420 A2	27/05/99	AU 1034799 A	07/06/99
		FI 105385 B	00/00/00
		FI 974133 A	05/05/99
WO 9837721 A2	27/08/98	AU 6216398 A	09/09/98
		CN 1251249 T	19/04/00
		EP 0962113 A	08/12/99
		FI 102500 B	00/00/00
		FI 970705 A	20/08/98
		FI 980351 A	20/08/98
		JP 2001511989 T	14/08/01
		ZA 9801325 A	08/09/98
		FI 3694 U	30/10/98
EP 1111952 A2	27/06/01	FI 992769 A	23/06/01
		JP 2001231082 A	24/08/01
		US 2001006552 A	05/07/01

3GPP TS 33.102 V5.0.0 (2002-06)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Security Architecture
(Release 5)

Keywords
Security, Architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword 6

1 Scope 7

2 References 7

3 Definitions, symbols abbreviations and conventions 8
3.1 Definitions 8
3.2 Symbols 9
3.3 Abbreviations 10
3.4 Conventions 10

4 Overview of the security architecture 11

5 Security features 12
5.1 Network access security 12
5.1.1 User identity confidentiality 12
5.1.2 Entity authentication 13
5.1.3 Confidentiality 13
5.1.4 Data integrity 13
5.1.5 Mobile equipment identification 14
5.2 Network domain security 14
5.2.1 Void 14
5.2.2 Void 14
5.2.3 Void 14
5.2.4 Fraud information gathering system 14
5.3 User domain security 14
5.3.1 User-to-USIM authentication 14
5.3.2 USIM-Terminal Link 14
5.4 Application security 15
5.4.1 Secure messaging between the USIM and the network 15
5.4.2 Void 15
5.4.3 Void 15
5.4.4 Void 15
5.5 Security visibility and configurability 15
5.5.1 Visibility 15
5.5.2 Configurability 15

6 Network access security mechanisms 16
6.1 Identification by temporary identities 16
6.1.1 General 16
6.1.2 TMSI reallocation procedure 16
6.1.3 Unacknowledged allocation of a temporary identity 16
6.1.4 Location update 17
6.2 Identification by a permanent identity 17
6.3 Authentication and key agreement 17
6.3.1 General 17
6.3.2 Distribution of authentication data from HE to SN 19
6.3.3 Authentication and key agreement 21
6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain 24
6.3.5 Re-synchronisation procedure 25
6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR 26
6.3.7 Length of authentication parameters 26
6.4 Local authentication and connection establishment 27
6.4.1 Cipher key and integrity key setting 27
6.4.2 Ciphering and integrity mode negotiation 27
6.4.3 Cipher key and integrity key lifetime 27
6.4.4 Cipher key and integrity key identification 28
6.4.5 Security mode set-up procedure 28

6.4.6 Signalling procedures in the case of an unsuccessful integrity check 30
6.4.7 Signalling procedure for periodic local authentication 30
6.4.8 Initialisation of synchronisation for ciphering and integrity protection 31
6.4.9 Emergency call handling 32
6.4.9.1 Security procedures applied 32
6.4.9.2 Security procedures not applied 32
6.5 Access link data integrity 32
6.5.1 General 32
6.5.2 Layer of integrity protection 33
6.5.3 Data integrity protection method 33
6.5.4 Input parameters to the integrity algorithm 34
6.5.4.1 COUNT-I 34
6.5.4.2 IK 34
6.5.4.3 FRESH 34
6.5.4.4 DIRECTION 35
6.5.4.5 MESSAGE 35
6.5.5 Integrity key selection 35
6.5.6 UIA identification 35
6.6 Access link data confidentiality 35
6.6.1 General 35
6.6.2 Layer of ciphering 36
6.6.3 Ciphering method 36
6.6.4 Input parameters to the cipher algorithm 36
6.6.4.1 COUNT-C 36
6.6.4.2 CK 37
6.6.4.3 BEARER 38
6.6.4.4 DIRECTION 38
6.6.4.5 LENGTH 38
6.6.5 Cipher key selection 38
6.6.6 UEA identification 38
6.7 Void 38
6.8 Interoperation and handover between UMTS and GSM 39
6.8.1 Authentication and key agreement of UMTS subscribers 39
6.8.1.1 General 39
6.8.1.2 R99+ HLR/AuC 40
6.8.1.3 R99+ VLR/SGSN 41
6.8.1.4 R99+ ME 42
6.8.1.5 USIM 42
6.8.2 Authentication and key agreement for GSM subscribers 43
6.8.2.1 General 43
6.8.2.2 R99+ HLR/AuC 43
6.8.2.3 VLR/SGSN 44
6.8.2.4 R99+ ME 44
6.8.3 Distribution and use of authentication data between VLRs/SGSNs 44
6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS 45
6.8.4.1 UMTS security context 46
6.8.4.2 GSM security context 46
6.8.5 Intersystem handover for CS Services – from GSM BSS to UTRAN 46
6.8.5.1 UMTS security context 47
6.8.5.2 GSM security context 47
6.8.6 Intersystem change for PS Services – from UTRAN to GSM BSS 47
6.8.6.1 UMTS security context 47
6.8.6.2 GSM security context 48
6.8.7 Intersystem change for PS services – from GSM BSS to UTRAN 48
6.8.7.1 UMTS security context 48
6.8.7.2 GSM security context 48

7 Void 49

8 Application security mechanisms 49
8.1 Void 49
8.2 Void 49

8.3 Mobile IP security 49

Annex A (informative): Requirements analysis 50

Annex B: Void 51

Annex C (informative): Management of sequence numbers 52

C.1 Generation of sequence numbers in the Authentication Centre 52
C.1.1 Sequence number generation schemes 52
C.1.1.1 General scheme 52
C.1.1.2 Generation of sequence numbers which are not time-based 53
C.1.1.3 Time-based sequence number generation 53
C.1.2 Support for the array mechanism 53

C.2 Handling of sequence numbers in the USIM 53
C.2.1 Protection against wrap around of counter in the USIM 54
C.2.2 Verification of sequence number freshness in the USIM 54
C.2.3 Notes 54

C.3 Sequence number management profiles 55
C.3.1 Profile 1: management of sequence numbers which are partly time-based 55
C.3.2 Profile 2: management of sequence numbers which are not time-based 56
C.3.3 Profile 3: management of sequence numbers which are entirely time-based 56
C.3.4 Guidelines for the allocation of the index values in the array scheme 57

C.4 Guidelines for interoperability in a multi-vendor environment 57

Annex D: Void 58

Annex E: Void 59

Annex F (informative): Example uses of AMF 60

F.1 Support multiple authentication algorithms and keys 60

F.2 Changing sequence number verification parameters 60

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys 60

Annex G (informative): Change history 61

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (TS 21.133 [1]) and implement the security objectives and principles described in TS 33.120 [2]. A security mechanism is an element that is used to realise a security feature. All security features and security mechanisms taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e. intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the MS are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

3 Definitions, symbols abbreviations and conventions

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101 [21], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905 [3]. 'User Equipment', 'USIM', 'SIM' and 'IC Card' have been defined in TS 22.201 [21].

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5).

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.

R99+ ME capable of UMTS AKA: either a R99+ UMTS only ME, a R99+ GSM/UMTS ME, or a R99+ GSM only ME that does support USIM-ME interface.

R99+ ME not capable of UMTS AKA: a R99+ GSM only ME that does not support USIM-ME interface.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MAC-S
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK in normal procedures
f5*	Key generating function used to compute AK in re-synchronisation procedures
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], for the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number
SQN_{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN_{MS}	The highest sequence number the USIM has accepted
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

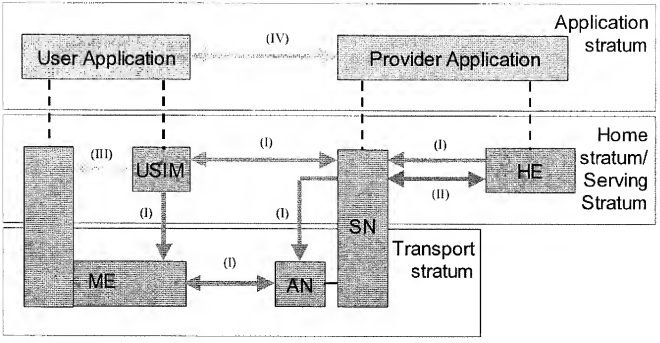


Figure 1: Overview of the security architecture

Five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations;
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 2 gives an overview of the ME registration and connection principles within UMTS with a CS service domain and a PS service domain. As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. In clause 6 the detailed procedures are defined and when not otherwise stated they are used in both service domains.

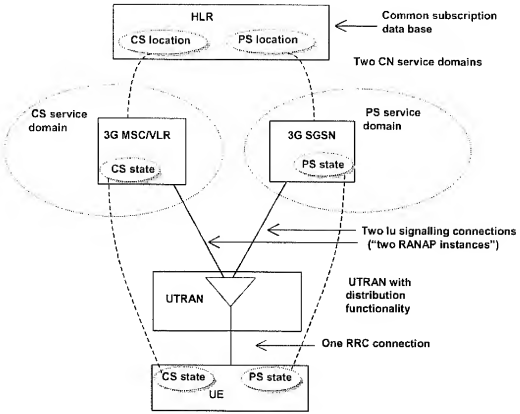


Figure 2: Overview of the ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G_SGSN and 3G GGSN, as the main serving nodes (Extract from TS 23.121 [4] – Figure 4-8)

5 Security features

5.1 Network access security

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

- **user identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

To achieve these objectives, the user is normally identified by a temporary identity by which he is known by the visited serving network. To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Clause 6.1 describes a mechanism that allows a user to be identified on the radio path by means of a temporary identity by which he is known in the visited serving network. This mechanism should normally be used to identify a user on the radio path in location update requests, service requests, detach requests, connection re-establishment requests, etc.

5.1.2 Entity authentication

The following security features related to entity authentication are provided:

- **user authentication:** the property that the serving network corroborates the user identity of the user;
- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

To achieve these objectives, it is assumed that entity authentication should occur at each connection set-up between the user and the network. Two mechanisms have been included: an authentication mechanism using an authentication vector delivered by the user's HE to the serving network, and a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

Clause 6.3 describes an authentication and key establishment mechanism that achieves the security features listed above and in addition establishes a secret cipher key (see 5.1.3) and integrity key (see 5.1.4) between the user and the serving network. This mechanism should be invoked by the serving network after a first registration of a user in a serving network and after a service request, location update request, attach request, detach request or connection re-establishment request, when the maximum number of local authentications using the derived integrity key have been conducted.

Clause 6.5 describes the local authentication mechanism. The local authentication mechanism achieves the security features user authentication and network authentication and uses an integrity key established between user and serving network during the previous execution of the authentication and key establishment procedure. This mechanism should be invoked by the serving network after a service request, location update request, attach request, detach request or connection re-establishment request, provided that the maximum number of local authentications using the same derived integrity key has not been reached yet.

5.1.3 Confidentiality

The following security features are provided with respect to confidentiality of data on the network access link:

- **cipher algorithm agreement:** the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently;
- **cipher key agreement:** the property that the MS and the SN agree on a cipher key that they may use subsequently;
- **confidentiality of user data:** the property that user data cannot be overheard on the radio access interface;
- **confidentiality of signalling data:** the property that signalling data cannot be overheard on the radio access interface;

Cipher key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Cipher algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected ciphering algorithm and the agreed cipher key to be applied in the way described in 6.6.

5.1.4 Data integrity

The following security features are provided with respect to integrity of data on the network access link:

- **integrity algorithm agreement:** the property that the MS and the SN can securely negotiate the integrity algorithm that they shall use subsequently;
- **integrity key agreement:** the property that the MS and the SN agree on an integrity key that they may use subsequently;

- **data integrity and origin authentication of signalling data:** the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed;

Integrity key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Integrity algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected integrity algorithm and the agreed integrity key to be applied in the way described in 6.4.

5.1.5 Mobile equipment identification

In certain cases, SN may request the MS to send it the mobile equipment identity of the terminal. The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls. The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI is not protected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

5.2 Network domain security

5.2.1 Void

5.2.2 Void

5.2.3 Void

5.2.4 Fraud information gathering system

NOTE: Some feature will be provided which will allow fraud information to be exchanged between 3GMS providers according to time constraints that yet have to be defined.

5.3 User domain security

5.3.1 User-to-USIM authentication

This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

This security feature is implemented by means of the mechanism described in TS 31.101 [5].

5.3.2 USIM-Terminal Link

This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal.

This security feature is implemented by means of the mechanism described in TS 22.022 [6].

5.4 Application security

5.4.1 Secure messaging between the USIM and the network

USIM Application Toolkit, as specified in TS 31.111 [15], provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

Security features for USIM Application Toolkit are implemented by means of the mechanisms described in TS 23.048 [7]. These mechanisms address the security requirements identified in TS 22.048 [16].

5.4.2 Void

5.4.3 Void

5.4.4 Void

5.5 Security visibility and configurability

5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up;
- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

5.5.2 Configurability

Configurability is the property that that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

6 Network access security mechanisms

6.1 Identification by temporary identities

6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile subscriber identity (TMSI/P-TMSI). A TMSI /P-TMSI has local significance only in the location area or routing area in which the user is registered. Outside that area it should be a accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

The TMSI/P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

The procedures and mechanisms are described in GSM 03.20 [8] and TS 23.060 [9]. The following sections contain a summary of this feature.

6.1.2 TMSI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new TMSI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 3.

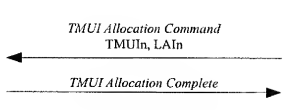


Figure 3: TMSI allocation

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (TMSIn) and stores the association of TMSIn and the permanent identity IMSI in its database. The TMSI should be unpredictable. The VLR then sends the TMSIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores TMSIn and automatically removes the association with any previously allocatedTMSI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMSIo and the IMSI (if there was any) from its database.

6.1.3 Unacknowledged allocation of a temporary identity

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity from the user, the network shall maintain the association between the new temporary identity TMSIn and the IMSI and between the old temporary identity TMSIo (if there is any) and the IMSI.

For a user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity TMSIo or the new temporary identity TMSIn. This allows the network to determine the temporary identity stored in the mobile station. The network shall subsequently delete the association between the other temporary identity and the IMSI, to allow the temporary identity to be allocated to another user.

For a network-originated transaction, the network shall identify the user by its permanent identity (IMSI). When radio contact has been established, the network shall instruct the user to delete any stored TMSI. When the network receives an acknowledgement from the user, the network shall delete the association between the IMSI and any TMSI to allow the released temporary identities to be allocated to other users.

Subsequently, in either of the cases above, the network may initiate the normal TMSI reallocation procedure.

Repeated failure of TMSI reallocation (passing a limit set by the operator) may be reported for O&M action.

6.1.4 Location update

In case a user identifies itself using a TMSIo/LAIo pair that was assigned by the visited VLRn the IMSI can normally be retrieved from the database. If this is not the case, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

In case a user identifies itself using a TMSIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRo exchange authentication data, the visited VLRn should request the previously visited VLRo to send the permanent user identity. This mechanism is described in 6.3.4, it is integrated in the mechanism for distribution of authentication data between VLRs. If the previously visited VLRo cannot be contacted or cannot retrieve the user identity, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

6.2 Identification by a permanent identity

The mechanism described in here allows the identification of a user on the radio path by means of the permanent subscriber identity (IMSI).

The mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity. In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the TMSI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.

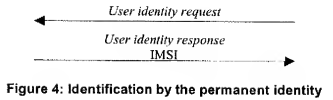


Figure 4: Identification by the permanent identity

The mechanism is initiated by the visited VLR/SGSN that requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality.

6.3 Authentication and key agreement

6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication. The sequence number SQN_{HE} is an individual counter for each user and the sequence number SQN_{MS} denotes the highest sequence number the USIM has accepted.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from ISO/IEC 9798-4 [10] (section 5.1.1).

An overview of the mechanism is shown in Figure 5.

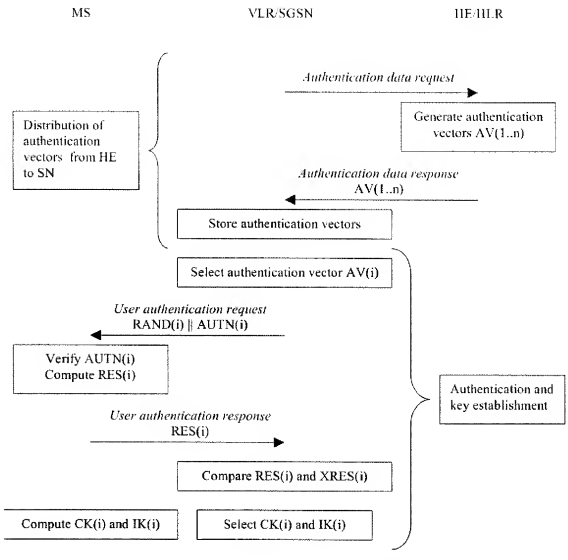


Figure 5: Authentication and key agreement

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the VLR/SGSN and the USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the ordered array and sends the parameters RAND and AUTN to the user. Authentication vectors in a particular node are used on a first-in / first-out basis. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the VLR/SGSN. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities which perform ciphering and integrity functions.

VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:

A procedure to distribute authentication information from the HE/AuC to the VLR/SGSN. This procedure is described in 6.3.2. The VLR/SGSN is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the VLR/SGSN to the HE/AuC are adequately secure. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the VLR/SGSN and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited VLR to the newly visited VLR. This procedure is described in 6.3.4. It is also assumed that the links between VLR/SGSNs are adequately secure.

6.3.2 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the VLR/SGSN with an array of fresh authentication vectors from the user's HE to perform a number of user authentications.

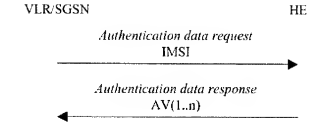


Figure 6: Distribution of authentication data from HE to VLR/SGSN

The VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC.

The *authentication data request* shall include the IMSI and the requesting node type (PS or CS).

Upon the receipt of the *authentication data request* from the VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n). The authentication vectors are ordered based on sequence number.

Figure 7 shows the generation of an authentication vector AV by the HE/AuC.

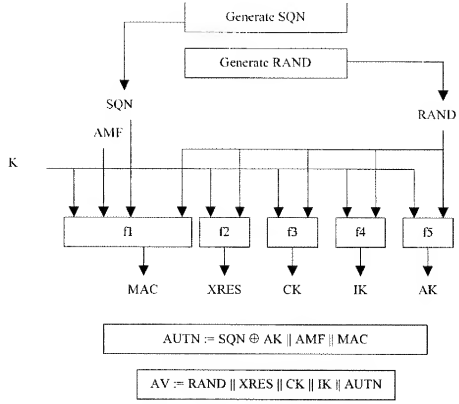


Figure 7: Generation of authentication vectors

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

For each user the HE/AuC keeps track of a counter: SQN_{HE}

The HE has some flexibility in the management of sequence numbers, but some requirements need to be fulfilled by the mechanism used:

a) The generation mechanism shall allow a re-synchronisation procedure in the HE described in section 6.3.5.

b) In case the SQN exposes the identity and location of the user, the AK may be used as an anonymity key to conceal it.

c) The generation mechanism shall allow protection against wrap around the counter in the USIM.
A method how to achieve this is given in informative Annex C.2.

The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last x = 32 sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.
The same minimum number x needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

The use of SQN_{HE} is specific to the method of generation sequence numbers. A method is specified in Annex C.1 how to generate a fresh sequence number. A method is specified in Annex C.2 how to verify the freshness of a sequence number.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of this field are included in Annex F.

Subsequently the following values are computed:

- a message authentication code $MAC = f1_K(SQN \| RAND \| AMF)$ where f1 is a message authentication function;
- an expected response $XRES = f2_K(RAND)$ where f2 is a (possibly truncated) message authentication function;
- a cipher key $CK = f3_K(RAND)$ where f3 is a key generating function;
- an integrity key $IK = f4_K(RAND)$ where f4 is a key generating function;
- an anonymity key $AK = f5_K(RAND)$ where f5 is a key generating function or $f5 = 0$.

Finally the authentication token $AUTN = SQN \oplus AK \| AMF \| MAC$ is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then $f5 = 0$ ($AK = 0$).

6.3.3 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

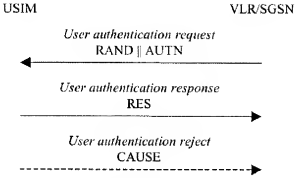


Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. Authentication vectors in a particular node are used on a first-in / first-out basis. The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

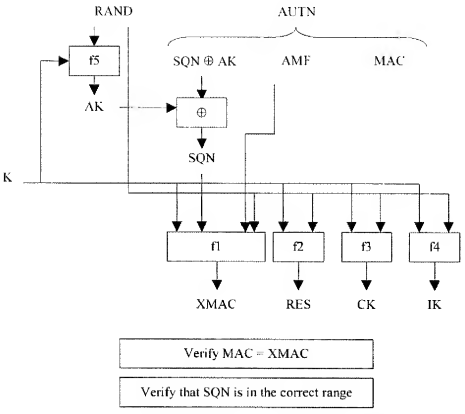


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. In this case, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the USIM considers the sequence number to be not in the correct range, it sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MAC-S. Conc(SQN_{MS}) = SQN_{MS} ⊕ $f5^*_K$(RAND) is the concealed value of the counter SQN_{MS} in the MS, and MAC-S = $f1^*_K$(SQN_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5, f5* and vice versa. f5* is the key generating function used to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of f5* about those of f1, f1*, f2, ... , f5 and vice versa.

The AMF used to calculate MAC-S assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

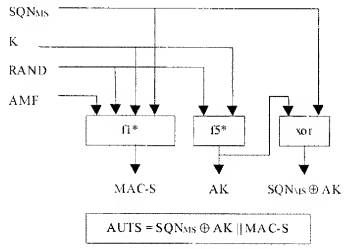


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the USIM computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. If the USIM also supports conversion function c3, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK until the next successful execution of AKA.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector. If XRES and RES are different, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Re-use and re-transmission of (RAND, AUTN)

The verification of the SQN by the USIM will cause the MS to reject an attempt by the VLR/SGSN to re-use a quintet to establish a particular UMTS security context more than once. In general therefore the VLR/SGSN shall use a quintet only once.

There is one exception however: in the event that the VLR/SGSN has sent out an *authentication request* using a particular quintet and does not receive a response message (*authentication response* or *authentication reject*) from the MS, it may re-transmit the *authentication request* using the same quintet. However, as soon as a response message arrives no further re-transmissions are allowed. If after the initial transmission or after a series of re-transmissions no response arrives, retransmissions may be abandoned. If retransmissions are abandoned then the VLR/SGSN shall delete the quintet. At the MS side, in order to allow this re-transmission without causing additional re-synchronisation procedures, the ME shall store for the PS domain (and optionally the CS domain) the last received RAND as well as the corresponding RES, CK and IK. If the USIM returned SRES and Kc (for GSM access), the ME shall store these values. When the ME receives an *authentication request* and discovers that a RAND is repeated, it shall re-transmit the response. The ME shall delete the stored values RAND, RES and SRES (if they exist) as soon as the 3G security mode command or the GSM cipher mode command is received by the ME or the connection is aborted. If the ME can handle the retransmission mechanism for CS domain then it shall be able to handle the retransmission for both PS and CS domain simultaneously.

6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited VLR/SGSN with temporary authentication data from a previously visited VLR/SGSN within the same serving network domain.

The procedure is shown in Figure 11.

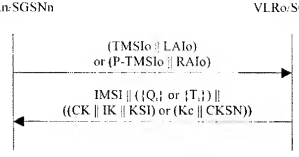


Figure 11: Distribution of IMSI and temporary authentication data within one serving network domain

The procedure shall be invoked by the newly visited VLRn/SGSNn after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited VLRo/SGSNo that belongs to the same serving network domain as the newly visited VLRn/SGSNn.

The protocol steps are as follows:

a) The VLRn/SGSNn sends a *user identity request* to the VLRo/SGSNo, this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).

b) The VLRo/SGSNo searches the user data in the database.

   If the user is found, the VLRo/SGSNo shall send a *user identity response* back that:

   i) shall include the IMSI,

   ii) may include a number of unused authentication vectors (quintets or triplets) ordered on a first-in / first-out basis, and

   iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

   The VLRo/SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

   If the user cannot be identified the VLRo/SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

c) If the VLRn/SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included.

   If the VLRn/SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.

6.3.5 Re-synchronisation procedure

A VLR/SGSN may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the VLR/SGSN sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters:

- *RAND* sent to the MS in the preceding user authentication request, and
- *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

An VLR/SGSN will not react to unsolicited "synchronisation failure indication" messages from the MS.

The VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves SQN_{MS} from Conc(SQN_{MS}) by computing Conc(SQN_{MS}) $\oplus$ $f5^*_K(RAND)$.
2. The HE/AuC checks if SQN_{HE} is in the correct range, i.e. if the next sequence number generated SQN_{HE} using would be accepted by the USIM.
3. If SQN_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3).
5. If the verification is successful the HE/AuC resets the value of the counter SQN_{HE} to SQN_{MS}.
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter SQN_{HE} was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SQN_{HE}. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. Figure 12 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in section 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this section).

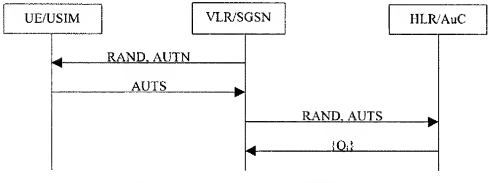


Figure 12: Resynchronisation mechanism

6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR

The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.

The procedure is shown in Figure 13.

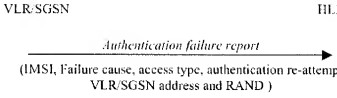


Figure 13: Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The *authentication failure report* shall contain:

1. Subscriber identity;
2. Failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong;
3. Access type. This indicates the type of access that initiated the authentication procedure;
4. Authentication re-attempt. This indicates whether the failure was produced in a normal authentication attempt or it was due to an authentication reattempt (there was a previous unsuccessful authentication);
5. VLR/SGSN address;
6. RAND. This number uniquely identifies the specific AV that failed authentication.

The HE may decide to cancel the location of the user after receiving an *authentication failure report* and may store the received data so that further processing to detect possible fraud situations could be performed.

6.3.7 Length of authentication parameters

The authentication key (K) shall have a length of 128 bits.

The random challenge (RAND) shall have a length of 128 bits.

Sequence numbers (SQN) shall have a length of 48 bits.

The anonymity key (AK) shall have a length of 48 bits.

The authentication management field (AMF) shall have a length of 16 bits.

The message authentication codes MAC in AUTN and MAC-S in AUTS shall have a length of 64 bits.

The cipher key (CK) shall have a length of 128 bits.

The integrity key (IK) shall have a length of 128 bits.

The authentication response (RES) shall have a variable length of 4-16 octets.

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

Authentication and key setting are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TMSI or IMSI) is known by the VLR/SGSN. The CK and IK are stored in the VLR/SGSN and transferred to the RNC when needed. The CK and IK for the CS domain are stored on the USIM and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the ME as part of the security mode set-up procedure (see 6.4.5) that follows the authentication procedure.

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the network have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the network are willing to use an unciphered connection, then an unciphered connection shall be used.

3) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement, which generates cipher/integrity keys, is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values $START_{CS}$ and $START_{PS}$ of the bearers that were protected in that RRC connection are compared with the maximum value, THRESHOLD. If $START_{CS}$ and/or $START_{PS}$ have reached the maximum value (THRESHOLD), the ME marks the START value in the USIM for the corresponding core network domain(s) as invalid by setting the $START_{CS}$ and/or $START_{PS}$ to THRESHOLD, deletes the cipher key and the integrity key stored on the USIM and sets the KSI to invalid (refer to section 6.4.4). Otherwise, the $START_{CS}$ and $START_{PS}$ are stored in the USIM. The maximum value THRESHOLD is set by the operator and stored in the USIM.

When the next RRC connection is established START values are read from the USIM. Then, the ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if $START_{CS}$ and/or $START_{PS}$ has reached the maximum value THRESHOLD, for the corresponding core network domain(s).

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

When the user is attached to a UTRAN, a R99+ ME with a SIM inserted shall use a default value for maximum value of $START_{CS}$ or $START_{PS}$ as described in section 6.8.2.4.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK. KSI in UMTS corresponds to CKSN in GSM. The USIM stores one KSI/CKSN for the PS domain key set and one KSI/CKSN for the CS domain key set.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

KSI and CKSN have the same format. The key set identifier is three bits. Seven values are used to identify the key set. A value of '111' is used by the mobile station to indicate that a valid key is not available for use. At deletion of the cipher key and integrity key, the KSI is set to '111'. The value '111' in the other direction from network to mobile station is reserved.

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement.

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

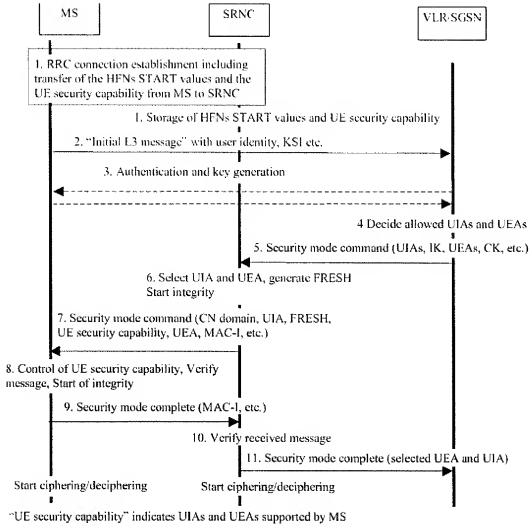


Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the UE. The RNC is monitoring the COUNT-C value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

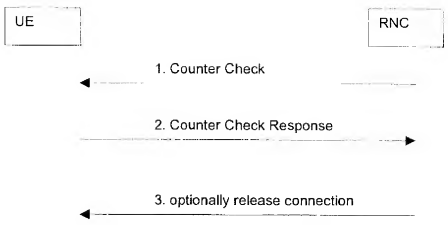


Figure 15a: RNC periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the RNC. The Counter Check message contains the most significant parts of the COUNT-C values (which reflect amount of data sent and received) from each active radio bearer.

2. The UE compares the COUNT-C values received in the Counter Check message with the values of its radio bearers. Different UE COUNT-C values are included within the Counter Check Response message.

3. If the RNC receives a counter check response message that does not contain any COUNT-C values, the procedure ends. If the RNC receives a counter check response that contains one or several COUNT-C values, the RNC may release the connection.

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the $START_{CS}$ and the $START_{PS}$ value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting $START_{CS}$ and $START_{PS}$ to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection) and the RLC SN (for ciphering) are initialised to 0.

During an ongoing radio connection, the $START_{CS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data radio bearers protected using CK_{CS} and/or IK_{CS}, incremented by 1, i.e.:

$START_{CS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{CS} and IK_{CS}}) + 1.

- If current $START_{CS} < START_{CS}'$ then $START_{CS} = START_{CS}'$, otherwise $START_{CS}$ is unchanged.

Likewise, during an ongoing radio connection, the $START_{PS}$ value in the ME and in the SRNC is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$START_{PS}' = MSB_{20}$ (MAX {COUNT-C, COUNT-I | all radio bearers (including signalling) protected with CK_{PS} and IK_{PS}}) + 1.

- If current $START_{PS} < START_{PS}'$ then $START_{PS} = START_{PS}'$, otherwise $START_{PS}$ is unchanged.

If any of the COUNT-C or COUNT-I assigned to the radio bearers of the same CN domain reaches its maximum value, the ME and SRNC shall set START of the corresponding CN domain to its maximum value.

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates $START_{CS}$ and $START_{PS}$ in the USIM with the current values.

During authentication and key agreement the START value associated with the new key set of the corresponding service domain is set to 0 in the USIM and in the ME.

6.4.9 Emergency call handling

PLMNs shall support an emergency call teleservice as defined in TS 22.003 which fulfils the additional service requirements defined in TS 22.101.

6.4.9.1 Security procedures applied

The security mode procedure shall be applied as part of emergency call establishment as defined in TS 24.008. Thus, integrity protection (and optionally ciphering) shall be applied as for a non-emergency call. If authentication of the (U)SIM fails for any reason, the emergency call shall proceed as in 6.4.9.2 d) below. Once the call is in progress with integrity protection (and optionally ciphering) applied, failure of integrity checking or ciphering is an unusual circumstance and must be treated in the same manner as other equipment failures, that is, the call will terminate.

6.4.9.2 Security procedures not applied

As a serving network option, emergency calls may be established without the network having to apply the security mode procedure as defined in TS 24.008.

The following are the only cases where the "security procedure not applied" option may be used:

a) Authentication is impossible because the (U)SIM is absent;

b) Authentication is impossible because the serving network cannot obtain authentication vectors due to a network failure;

c) Authentication is impossible because the (U)SIM is not permitted to receive non-emergency services from the serving network (e.g. there is no roaming agreement or the IMSI is barred);

d) Authentication is possible but the serving network cannot successfully authenticate the (U)SIM.

6.5 Access link data integrity

6.5.1 General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ME and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).

All signalling messages except the following ones shall then be integrity protected:

HANDOVER TO UTRAN COMPLETE

PAGING TYPE 1

PUSCH CAPACITY REQUEST

PHYSICAL SHARED CHANNEL ALLOCATION

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

RRC CONNECTION RELEASE (CCCH only)

SYSTEM INFORMATION (BROADCAST INFORMATION)

SYSTEM INFORMATION CHANGE INDICATION

TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

6.5.2 Layer of integrity protection

The UIA shall be implemented in the ME and in the RNC.

Integrity protection shall be applied at the RRC layer.

6.5.3 Data integrity protection method

Figure 16 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signalling message.

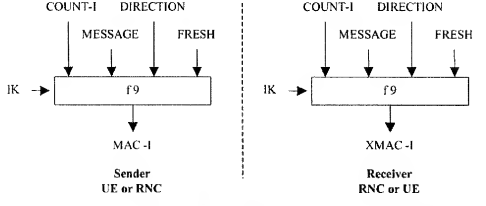


Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (COUNT-I), a random value generated by the network side (FRESH), the direction bit DIRECTION and the signalling data MESSAGE. Based on these input parameters the user computes message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

For signalling radio bearers (RB 0-4) there is one COUNT-I value per up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. The "short" sequence number is the 4-bit RRC sequence number (RRC SN) that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.

Figure 16a: The structure of COUNT-I

The RRC HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.5.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that a valid IK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM are not up-to-date or $START_{CS}$ or $START_{PS}$ have reached THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSNas part of a quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) *security mode command*.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it to the ME in the RRC message that indicates a new UTRAN Radio Network Temporary Identity due to a SRNC relocation (see TS 25.331 [17]).

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of radio bearers for user data is not protected.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode command from the VLR/SGSN.

NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.5.6 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the integrity protection function f9 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and should be confidentiality protected. To ensure identity confidentiality (see section 6.1), the temporary user identity (P-)TMSI should be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ME and the RNC.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- If a radio bearer is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a radio bearer is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the ME.

6.6.3 Ciphering method

Figure 16b illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the keystream. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

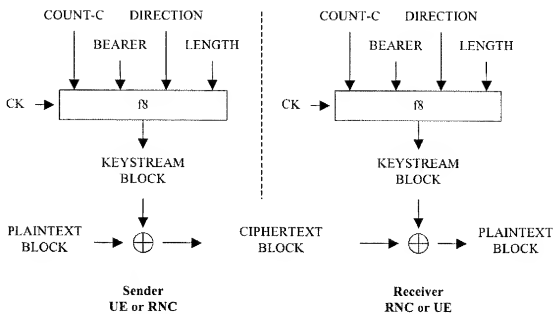


Figure 16b: Ciphering of user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the cipher key CK, a time dependent input COUNT-C, the bearer identity BEARER, the direction of transmission DIRECTION and the length of the keystream required LENGTH. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. For all transparent mode RLC radio bearers of the same CN domain COUNT-C is the same, and COUNT-C is also the same for uplink and downlink.

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

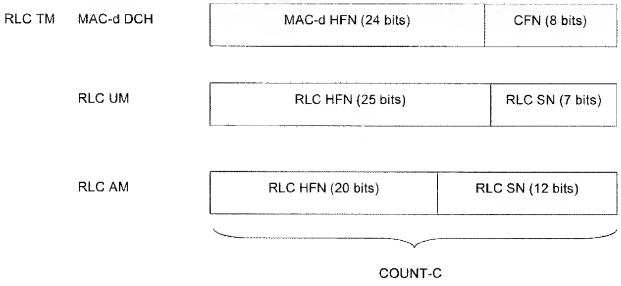


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.
- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. The "long" sequence number is the 25-bit RLC UM HFN which is incremented at each RLC SN cycle.
- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number (RLC SN) and this is part of the RLC AM PDU header. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in section 6.4.8. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START. The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

When a new radio bearer is created during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see section 6.4.8).

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. The CK to use for a particular radio bearer is described in 6.6.5. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that a valid CK is available. The ME shall trigger a new authentication procedure if the current value of $START_{CS}$ or $START_{PS}$ in the USIM have reached THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR/SGSN and stored in the VLR/SGSN as part of the quintet. It is sent from the VLR/SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The radio bearers for CS user data are ciphered with CK_{CS}.

The radio bearers for PS user data are ciphered with CK_{PS}.

The signalling radio bearers are used for transfer of signalling data for services delivered by both CS and PS service domains. These signalling radio bearers are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection has to be changed, when a new connection is established with another service domain, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed by the RNC within five seconds after receiving the security mode command from the VLR/SGSN.

NOTE: For the behaviour of the terminal regarding key changes see section 6.4.5.

6.6.6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.7 Void

6.8 Interoperation and handover between UMTS and GSM

6.8.1 Authentication and key agreement of UMTS subscribers

6.8.1.1 General

For UMTS subscribers, authentication and key agreement will be performed as follows:

- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ ME capable of UMTS AKA and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ ME not capable of UMTS AKA or R98- ME or R98- ME. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.

NOTE: To operate within a R99+ ME not capable of UMTS AKA or R98- ME, the USIM may support the SIM-ME interface as defined in GSM 11.11, and support GSM AKA which provides the corresponding GSM functionality for calculating SRES and Kc based on the authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the UMTS authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2.

- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the VLR/SGSN is R98-. In this case, the USIM derives the GSM user response SRES and the GSM cipher key Kc from the UMTS user response RES and the UMTS cipher/integrity keys CK, IK.

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 18 shows the different scenarios that can occur with UMTS subscribers in a mixed network architecture.

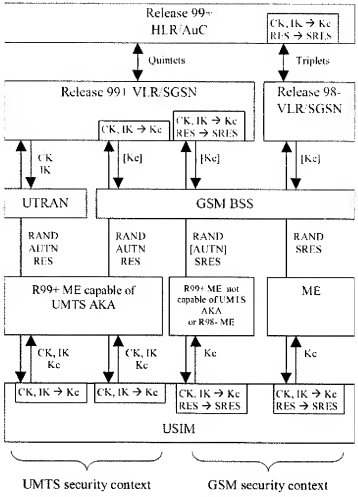


Figure 18: Authentication and key agreement of UMTS subscribers

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send quintets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintets using the following conversion functions:

a) c1: $RAND_{[GSM]} = RAND$

b) c2: $SRES_{[GSM]} = XRES^*_1 \text{ xor } XRES^*_2 \text{ xor } XRES^*_3 \text{ xor } XRES^*_4$

c) c3: $Kc_{[GSM]} = CK_1 \text{ xor } CK_2 \text{ xor } IK_1 \text{ xor } IK_2$

whereby XRES* is 16 octets long and XRES* = XRES if XRES is 16 octets long and XRES* = XRES || 0...0 if XRES is shorter than 16 octets, XRES*, are all 4 octets long and $XRES^* = XRES^*_1 \,||\, XRES^*_2 \,||\, XRES^*_3 \,||\, XRES^*_4$, CK_i and IK_i are both 64 bits long and $CK = CK_1 \,||\, CK_2$ and $IK = IK_1 \,||\, IK_2$

6.8.1.3 R99+ VLR/SGSN

The AKA procedure will depend on the terminal capabilities, as follows:

UMTS subscriber with R99+ ME

When the user has R99+ ME, the VLR/SGSN shall send the ME a UMTS authentication challenge (i.e. RAND and AUTN) using a quintet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited R99+ VLR/SGSN.

Note: Originally all quintets are provided by the HLR/AuC.

When the R99+ ME is capable of the USIM-ME interface UMTS AKA is performed and the VLR/SGSNreceives the UMTS response RES.

UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in theVLR/SGSN.

When the user is attached to a UTRAN, the UMTS cipher/integrity keys are sent to the RNC, where the cipher/integrity algorithms are allocated.

When the user is attached to a GSM BSS, UMTS AKA is followed by the derivation of the GSM cipher key from the UMTS cipher/integrity keys. When the user receives service from an MSC/VLR, the derived cipher key Kc is then sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS authentication and key freshness is always provided to UMTS subscribers with R99+ ME independently of the radio access network.

When the R99+ ME is not capable of the USIM-ME interface GSM AKA is performed and the VLR/SGSN receives the GSM response SRES.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

The R99+ VLR/SGSN shall reject authentication if SRES is received in response of a UMTS challenge (RAND, AUTN) over an Iu-Interface.

The R99+ VLR/SGSN shall accept authentication if a valid SRES is received in response of a UMTS challenge (RAND, AUTN) over A or Gb-Interface. This will happen in case a UICC is inserted in a R99+ ME that is not capable of UMTS AKA and is attached to a GSM BSS. In this case the R99+ VLR/SGSN uses function c2 to convert RES (from the quintet) to SRES to verify the received SRES.

UMTS subscriber with R98- ME

When the user has R98- ME, the R99+ VLR/SGSN send the ME a GSM authentication challenge using a triplet that is either:

a) derived by means of the conversion functions c2 and c3 in the R99+ VLR/SGSN from a quintet that is:

i) retrieved from the local database,

ii) provided by the HLR/AuC, or

iii) provided by the previously visited R99+ VLR/SGSN, or

b) provided as a triplet by the previously visited VLR/SGSN.

NOTE: R99+ VLR/SGSN will always provide quintets for UMTS subscribers.

NOTE: For a UMTS subscriber, all triplets are derived from quintets, be it in the HLR/AuC or in an VLR/SGSN.

GSM AKA results in the establishment of a GSM security context: the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

In this case the user is attached to a GSM BSS. When the user receives service from an MSC/VLR, the GSM cipher key is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS authentication and key freshness cannot be provided to UMTS subscriber with R98- ME.

6.8.1.4 R99+ ME

Release 99+ ME that has UTRAN radio capability shall support the USIM-ME interface as specified in TS 31.102 [20].

Release 99+ ME that has no UTRAN radio capabilities may support the USIM-ME interface as specified in TS 31.102 [20].

R99+ ME capable of UMTS AKA with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

R99+ ME capable of UMTS AKA with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

A R99+ ME that does not support the USIM-ME interface (not capable of UMTS AKA) with a USIM inserted can only participate in GSM AKA.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are passed to the ME. If the USIM supports conversion function c3 and/or GSM AKA, the ME shall also receive a GSM cipher key Kc derived at the USIM.

The execution of GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ME.

6.8.1.5 USIM

The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

Feature 1: GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;

Feature 2: GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using R99+ ME not capable of UMTS AKA or R98- ME;

Feature 3: SIM-ME interface (GSM 11.11) to operate within R98- ME or R99+ ME not capable of UMTS AKA.

When the ME provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM shall store CK and IK as current security context data. If the USIM supports access to GSM cipher key derivation (feature 1), the USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the R99+ ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the R99+ ME.

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. The USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then stores the GSM cipher key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the R99+ ME shall be informed. A USIM that does not support GSM cipher key derivation (Feature 1) cannot operate in any GSM BSS. A USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN or in a both R99+ ME that is not capable of UMTS AKA.and in R98- ME.

6.8.2 Authentication and key agreement for GSM subscribers

6.8.2.1 General

For GSM subscribers, GSM AKA shall always be used.

The execution of the GSM AKA results in the establishment of a GSM security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc by the ME and the VLR/SGSN, both R99+ entities.

Figure 19 shows the different scenarios that can occur with GSM subscribers using either R98- or R99+ ME in a mixed network architecture.

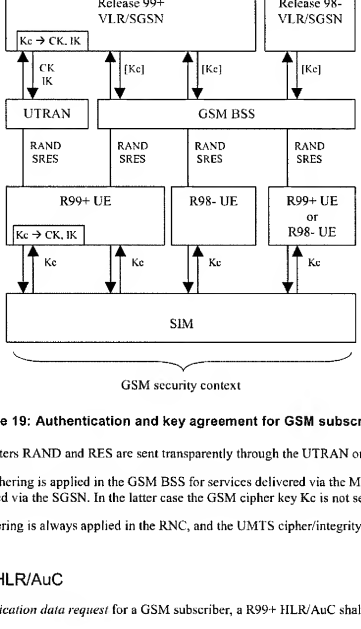


Figure 19: Authentication and key agreement for GSM subscribers

Note that the GSM parameters RAND and RES are sent transparently through the UTRAN or GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.2.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* for a GSM subscriber, a R99+ HLR/AuC shall send triplets generated as specified in GSM 03.20.

6.8.2.3 VLR/SGSN

The R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited VLR/SGSN.

NOTE: All triplets are originally provided by the HLR/AuC.

GSM AKA results in the establishment of a GSM security context: the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

When the user is attached to a UTRAN, the R99+ VLR/SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) c4: $CK_{[UMTS]} = Kc \parallel Kc$;

b) c5: $IK_{[UMTS]} = Kc_1 \text{ xor } Kc_2 \parallel Kc \parallel Kc_1 \text{ xor } Kc_2$;

whereby in c5, Kc, are both 32 bits long and $Kc = Kc_1 \parallel Kc_2$.

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the cipher key Kc is applied in the SGSN itself.

6.8.2.4 R99+ ME

R99+ ME with a SIM inserted, shall participate only in GSM AKA.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ME.

When the user is attached to a UTRAN, R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc using the conversion functions c4 and c5. The ME shall handle the $START_{CS}$ and $START_{PS}$ as described in section 6.4.8 with the exception that the START values are stored on the ME rather than on the GSM SIM. If the ME looses the current START value for a particular domain (e.g. due to power off) it shall delete the corresponding GSM cipher key (Kc), the derived UMTS cipher/integrity keys (CK and IK), and reset the START value to zero. The ME shall then trigger a new authentication and key agreement at the next connection establishment by indicating to the network that no valid keys are available for use using the procedure described in section 6.4.4.

When the user is attached to a UTRAN, a R99+ ME with a SIM inserted shall use a default value of all ones for maximum value of $START_{CS}$ or $START_{PS}$. The ME shall handle the maximum value of $START_{CS}$ or $START_{PS}$ as described in section 6.4.3 with the exception that the maximum value of $START_{CS}$ or $START_{PS}$ is stored on the ME rather than on the GSM SIM.

6.8.3 Distribution and use of authentication data between VLRs/SGSNs

The distribution of authentication data (unused authentication vectors and/or current security context data) between R99+ VLRs/SGSNs of the same service network domain is performed according to chapter 6.3.4. The following four cases are distinguished related to the distribution of authentication data between VLRs/SGSNs (of the same or different releases). Conditions for the distribution of such data and for its use when received at VLRn/SGSNn are indicated for each case:

a) R99+ VLR/SGSN to R99+ VLR/SGSN

UMTS and GSM authentication vectors can be distributed between R99+ VLRs/SGSNs. Note that originally all authentication vectors (quintets for UMTS subscribers and triplets for GSM subscribers) are provided by the HLR/AuC.

Current security context data can be distributed between R99+ VLRs/SGSNs. VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of ME release (R'99 ME ←→ R'98 ME) when the user registers at VLRn/SGSNn.

ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 ME (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

b) R98- VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed between R98- VLRs/SGSNs. Note that originally for GSM subscribers, triplets are generated by HLR/AuC and for UMTS subscribers, they are derived from UMTS authentication vectors by R99+ HLR/AuC. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

Since only GSM security context can be established under R98- SGSNs, security context data can be distributed and used between R98- SGSNs.

c) R99+ VLR/SGSN to R98- VLR/SGSN

R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM subscribers or can derive triplets from stored quintets originally provided by R99+ HLR/AuC for UMTS subscribers. Note that R98- VLR/SGSN can only establish GSM security context.

R99+ VLRs shall not distribute current security context data to R98- VLRs.

Since R98- SGSNs are only prepared to handle GSM security context data, R99+ SGSNs shall only distribute GSM security context data (Kc, CKSN) to R98- SGSNs.

d) R98- VLR/SGSN to R99+ VLR/SGSN.

In order to not establish a GSM security context for a UMTS subscriber, triplets provided by a R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context under GSM-BSS with a R98- ME.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintets) to HE. In the event, the R99+ VLR/SGSN receives quintets, it shall discard the triplets provided by the R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

R98- SGSNs can distribute GSM security context data only. The use of this information at R99+ SGSNn shall be performed according to the conditions stated in a).

6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode. The RNC may request the MS to send the MS Classmarks 2 and 3 which include information on the GSM ciphering algorithm capabilities of the MS. This is necessary only if the MS Classmarks 2 and 3 were not transmitted from UE to UTRAN during the RRC Connection Establishment. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5. The GSM BSS includes the selected GSM ciphering mode in the handover command message sent to the MS via the RNC.

The integrity protection of signalling messages is stopped at handover to GSM BSS.

The START values (see section 6.4.8) shall be stored in the ME/USIM at handover to GSM BSS.

6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a R99+ ME that is capable of UMTS AKA. At the network side, three cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and sends Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by other R98- MSC/VLR, the initial MSC/VLR derives the GSM cipher key from the stored UMTS cipher/integrity keys (using the conversion function c3) and sends it to the target BSC via the new MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

c) In case of a handover to a GSM BSS controlled by another R99+ MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR store the keys and sends the received GSM cipher key Kc to the target BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a R99+ ME. At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR sends the stored GSM cipher key Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR (R99+ or R98-), the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the new MSC/VLR controlling the target BSC. The initial MSC/VLR remains the anchor point throughout the service.

If the non-anchor MSC/VLR is R99+, then the anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the UMTS cipher/integrity keys CK and IK. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ME applies the stored GSM cipher key Kc.

6.8.5 Intersystem handover for CS Services – from GSM BSS to UTRAN

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, START value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM BSS to the new RNC, and to continue the communication in ciphered mode. The GSM BSS requests the MS to send the UMTS capability information, which includes information on the START values and UMTS security capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA. The target UMTS RNC includes the selected UMTS ciphering mode in the handover to UTRAN command message sent to the MS via the GSM BSS.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS. The UE security capability information, that has been sent from MS to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to MS and then verified by the MS (i.e. verified that it is equal to the UE security capability information stored in the MS).

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ ME that is capable of UMTS AKA under GSM BSS controlled by a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new RNC via the new MSC/VLR that controls the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

The anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the GSM cipher key Kc. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ME applies the stored UMTS cipher/integrity keys CK and IK.

6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is possible for a GSM subscriber with a R99+ ME or for a UMTS subscriber with a R99+ ME when the initial MSC/VLR is R98-. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the target RNC. In case of subsequent handover in a non-anchor R99+ MSC/VLR, a GSM cipher key Kc is received for a UMTS subscriber if the anchor MSC/VLR is R98-.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR (R99+ or R98-) sends the stored GSM cipher key Kc to the new MSC/VLR controlling the target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

At the user side, in either case, the ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them.

6.8.6 Intersystem change for PS Services – from UTRAN to GSM BSS

6.8.6.1 UMTS security context

A UMTS security context in UTRAN is only established for UMTS subscribers. At the network side, three cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

b) In case of an intersystem change to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

c) In case of an intersystem change to a GSM BSS controlled by a R98- SGSN, the initial SGSN derives the GSM cipher key Kc and sends the GSM cipher key Kc to the new SGSN. The new SGSN stores the GSM cipher key Kc and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in all cases, the ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

6.8.6.2 GSM security context

A GSM security context in UTRAN is only established for GSM subscribers. At the network side, two cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.

b) In case of an intersystem change to a GSM BSS controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the BSC. The new SGSN stores the key and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in both cases, the ME applies the GSM cipher key Kc that is stored.

6.8.7 Intersystem change for PS services – from GSM BSS to UTRAN

6.8.7.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ ME that is capable of UMTS AKA and connected to a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of an intersystem change to a UTRAN controlled by another SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the target RNC.

At the user side, in both cases, the ME applies the stored UMTS cipher/integrity keys CK and IK.

6.8.7.2 GSM security context

A GSM security context in GSM BSS can be either:

- **Established for a UMTS subscriber**

  A GSM security context for a UMTS subscriber is established in case the user has a R98- ME or R99+ ME not capable of UMTS AKA, where intersystem change to UTRAN is not possible, or in case the user has a R99+ ME but the SGSN is R98-, where intersystem change to UTRAN implies a change to a R99+ SGSN.

  As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the stored GSM cipher key Kc to the new SGSN controlling the target RNC.

  Since the new R99+ SGSN has no indication of whether the subscriber is GSM or UMTS, a R99+ SGSN shall perform a new UMTS AKA when receiving Kc from a R98- SGSN. A UMTS security context using fresh quintets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

  At the user side, new keys shall be agreed during the new UMTS AKA initiated by the R99+ SGSN.

- **Established for a GSM subscriber**

  Handover from GSM BSS to UTRAN for GSM subscriber is only possible with R99+ ME. At the network side, three cases are distinguished:

  a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the target RNC.

  b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC.

c) In case of an intersystem change from an R98-SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. To ensure use of UMTS keys for a possible UMTS subscriber (superfluous in this case), a R99+ SGSN will perform a new AKA when a R99+ ME is coming from a R98-SGSN.

At the user side, in all cases, the ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them. In case c) these keys will be over-written with a new CK, IK pair due to the new AKA.

7 Void

8 Application security mechanisms

8.1 Void

8.2 Void

8.3 Mobile IP security

The introduction of Mobile IP functionality for end users in 3G has no influence on the security architecture for 3G.

Mobile IP terminals may be equipped with security functionality independent of the 3G network access security in order to allow security functions outside the 3G network.

3G networks, supporting Mobile IP services, should support its inherent security functionality.

On the other hand, 3G network access security architecture can not be influenced or reduced by the Mobile IP option.

The Mobile IP security functionality must thus be separate from the 3G network access security and it is developed in an other forum, IETF.

Annex A (informative): Requirements analysis

[In this part of the document we will address the question "do the features meet the requirements?"]

Annex B:
Void

Annex C (informative): Management of sequence numbers

This annex is devoted to the management of sequence numbers for the authentication and key agreement protocol.

C.1 Generation of sequence numbers in the Authentication Centre

C.1.1 Sequence number generation schemes

C.1.1.1 General scheme

According to section 6.3 of this specification, authentication vectors are generated in the authentication centre (AuC) using sequence numbers. This section specifies how these sequence numbers are generated. Authentication vectors may be generated and sent by the AuC in batches. The sequence numbers for the authentication vectors in a batch are generated one after the other according to the process described below.

(1) In its binary representation, the sequence number consists of two concatenated parts $SQN = SEQ \parallel IND$. *IND* is an index used in the array scheme described in C.1.2 and C.2.2. *SEQ* in its turn consists of two concatenated parts $SEQ = SEQ1 \parallel SEQ2$. *SEQ1* represents the most significant bits of *SEQ*, and *SEQ2* represents the least significant bits of *SEQ*. *IND* represents the least significant bits of *SQN*.

(2) There is a counter SQN_{HE} in the HE. *SQN* is stored by this counter. SQN_{HE} is an individual counter, i.e. there is one per user. We have $SQN_{HE} = SEQ_{HE} \parallel IND_{HE}$.

(3) There is a global counter, e.g. a clock giving universal time. For short we call the value of this global counter at any one time *GLC*. If *GLC* is taken from a clock it is computed mod p, where $p = 2^n$ and n is the length of *GLC* and of *SEQ2* in bits.

(4) If *GLC* is taken from a clock then there is a number $D > 0$ such that the following holds:
(i) the time interval between two consecutive increases of the clock (the clock unit) shall be chosen such that, for each user, at most *D* batches are generated at the AuC during any *D* clock units;
(ii) the clock rate shall be significantly higher than the average rate at which batches are generated for any user;
(iii) $D << 2^n$.

(5) When the HE needs new sequence numbers *SQN* to create a new batch of authentication vectors, HE retrieves the (user-specific) value of $SEQ_{HE} = SEQ1_{HE} \parallel SEQ2_{HE}$ from the database.
(i) If $SEQ2_{HE} < GLC < SEQ2_{HE} + p - D + 1$ then HE sets $SEQ = SEQ1_{HE} \parallel GLC$;
(ii) if $GLC \leq SEQ2_{HE} \leq GLC + D - 1$ or $SEQ2_{HE} + p - D + 1 \leq GLC$ then HE sets $SEQ = SEQ_{HE} + 1$;
(iii) if $GLC + D - 1 < SEQ2_{HE}$ then HE sets $SEQ = (SEQ1_{HE} + 1) \parallel GLC$.
(iv) After the generation of the authentication vector has been completed SEQ_{HE} is reset to *SEQ*;
(v) for the handling of *IND* see C.1.2.

NOTES

1. The clock unit and the value *D* have to be chosen with care so that condition (4)(i) is satisfied for every user at all times. Otherwise, user identity confidentiality may be compromised. When the parameters are chosen appropriately sequence numbers for a particular user do not reveal significant information about the user's identity.
If authentication vectors for the CS and the PS domains are not separated by other means it is recommended to choose $D > 1$ as requests from the two different domains may arrive completely independently.

2. By setting the parameters in C.1.1.1 (1) to (5) in an appropriate way the general scheme specified in this subsection also includes the cases where either SEQ2 is void and SEQ = SEQ1 or else, SEQ1 is void and SEQ = SEQ2, as follows:
   (a) If SEQ2 is void the generation of sequence numbers is not time-based. We then formally set SEQ2 ≡ GLC ≡ 0 (identical to zero) and D = 1. Conditions (4)(i) to (iii) do not apply as there is no clock. Then (5)(ii) always holds, and SEQ is incremented by 1 at each request. For better readability, this case is separated out in C.1.1.2.
   (b) If SEQ1 is void then we set D = 1. Assuming a start condition $SEQ2_{HE} < GLC$ and the absence of failures in the AuC, the condition (5)(i) then always holds, and SEQ = GLC for each request, i.e. the generation of sequence numbers is entirely time-based. In order to also accommodate potential failures in the AuC for entirely time-based sequence number , the variant described in the following Annex C.1.1.3 may be used.

C.1.1.2 Generation of sequence numbers which are not time-based

The HE/AuC shall maintain a counter for each user, $SQN_{HE} = SEQ_{HE} \parallel IND_{HE}$. To generate a fresh sequence number, SEQ_{HE} is incremented by 1, and the new counter value is used to generate the next authentication vector. For the handling of *IND* see C.1.2.

C.1.1.3 Time-based sequence number generation

In its binary representation, the sequence number consists of two concatenated parts $SQN = SEQ \parallel IND$. The part *SEQ* is not divided into two parts. The global counter *GLC* is thus as long as *SEQ*. Instead of storing the individual counter SEQ_{HE} in the HE there is a value *DIF* stored in the HE which is individual for each user. The *DIF* value represents the current difference between generated *SEQ* values for that user and the *GLC*.

When the HE needs new sequence numbers *SQN* to create new authentication vectors, HE retrieves the (user-specific) value of *DIF* from the data base and calculates *SEQ* values as $SEQ = GLC + DIF$.

The *DIF* value may have to be updated in the HE only during the re-synchronization procedure. In this case the DIF value is set as $DIF = SEQ_{MS} - GLC$ where $SQN_{MS} = SEQ_{MS} \parallel IND_{MS}$ is the value sent by USIM in the re-synchronization procedure.

C.1.2 Support for the array mechanism

This subsection applies to all three schemes presented in subsection C.1.1.

Each time an authentication vector is generated, the AuC shall retrieve IND_{HE} from storage and allocate a new index value *IND* for that vector according to suitable rules and include it in the appropriate part of *SQN*. The index value may range from 0 to a -1 where a is the size of the array.

An example value for the array size a is given in Annex C.3.
The exact rules for index allocation are left unspecified. Guidelines are given in Annex C.3.4.

C.2 Handling of sequence numbers in the USIM

This section assumes that sequence numbers are generated according to Annex C.1.

The USIM keeps track of an array of sequence number values it has accepted. Let $SQN_{MS} = SEQ_{MS} \parallel IND_{MS}$ denote the highest sequence number in the array.

C.2.1 Protection against wrap around of counter in the USIM

The USIM will not accept arbitrary jumps in sequence numbers, but only increases by a value of at most Δ.

Therefore (before applying the freshness conditions of Annex C.2.2) the received sequence number SQN shall only be accepted by the USIM if $SEQ\text{-}SEQ_{MS} \leq \Delta$. If SQN can not be accepted then the USIM shall generate a synchronisation failure message using SQN_{MS}.

Conditions on the choice of Δ:

(1) Δ shall be sufficiently large so that the MS will not receive any sequence number with $SEQ - SEQ_{MS} > \Delta$ if the HE/AuC functions correctly.

(2) In order to prevent that SEQ_{HE} ever reaches the maximum batch number value *SEQmax* during the lifetime of the USIM the minimum number of steps $SEQmax / \Delta$ required to reach *SEQmax* shall be sufficiently large.

C.2.2 Verification of sequence number freshness in the USIM

The USIM shall maintain an array of a previously accepted sequence number components: $SEQ_{MS}(0)$, $SEQ_{MS}(1)$,… $SEQ_{MS}(a\text{-}1)$. The initial sequence number value in each array element shall be zero.

To verify that the received sequence number *SQN* is fresh, the USIM shall compare the received *SQN* with the sequence number in the array element indexed using the index value *IND* contained in *SQN*, i.e. with the array entry $SEQ_{MS}(i)$ where i = *IND* is the index value.

(a) If $SEQ > SEQ_{MS}(i)$ the USIM shall consider the sequence number to be guaranteed fresh and subsequently shall set $SEQ_{MS}(i)$ to *SEQ*.

(b) If $SEQ \leq SEQ_{MS}(i)$ the USIM shall generate a synchronisation failure message using the highest previously accepted sequence number anywhere in the array, i.e. SQN_{MS}.

The USIM shall also be able to put a limit L on the difference between SEQ_{MS} and a received sequence number component *SEQ*. If such a limit L is applied then, before verifying the above conditions (a) and (b), the sequence number shall only be accepted by the USIM if $SEQ_{MS} - SEQ < L$. If *SQN* can not be accepted then the USIM shall generate a synchronisation failure message using SQN_{MS}.

C.2.3 Notes

1. Using the above array mechanism, it is not required that a previously visited VLR/SGSN deletes the unused authentication vectors when a user de-registers from the serving network (super-charger concept). Retaining the authentication vectors for use when the user returns later may be more efficient as regards signalling when a user abroad switches a lot between two serving networks.

2. The array mechanism may also be used to avoid unjustified rejection of user authentication requests when authentication vectors in two VLR/SGSNs from different mobility management domains (circuit and packet) are used in an interleaving fashion.

3. When a VLR/SGSN uses fresh authentication vectors obtained during a previous visit of the user, the USIM can reject them although they have not been used before (because the array size a and the age limit L are finite). Rejection of a sequence number can therefore occur in normal operation, i.e., it is not necessarily caused by (malicious) replay or a database failure.

4. The mechanism presented in this section may allow the USIM to exploit knowledge about which authentication vectors were sent to the same VLR/SGSN. It may be assumed that authentication vectors sent to the same VLR/SGSN are always used in the correct order. Consequently, only one sequence number among those sent to the same VLR/SGSN has to be stored.

5. With the exception of SQN_{MS}, the entries of the array need not be stored in full length if a limit L (age limit) on the difference between SEQ_{MS} and a received sequence number component *SEQ* is applied.

6. Condition (2) of Annex C.2.1 on Δ means that SQN_{MS} can reach its maximum value only after a minimum of $SEQmax / \Delta$ successful authentications have taken place.

7. There is a dependency of the choice of Δ and the size n of global counter GLC in Annex C.1.1.1: Δ shall be chosen larger than 2^n.

C.3 Sequence number management profiles

This section provides examples how values for the parameters defined in sections C.1 and C.2 may be chosen in a coherent way. These examples may serve as references when specifying practical sequence number management schemes. There is one example set of values for each of the three types of sequence number generation schemes:

- partly time-based corresponding to Annex C.1.1.1;
- not time-based corresponding to Annex C.1.1.2;
- entirely time-based corresponding to Annex C.1.1.3.

C.3.1 Profile 1: management of sequence numbers which are partly time-based

Generation of sequence numbers:

This follows the general scheme for the generation of sequence numbers specified in Annex C.1.1.1. The following parameter values are suggested for reference:

Time unit of the clock: 1 second

Length of IND in bits = n : 24
This means that GLC will wrap around after $p = 2^n = 2^{24}$ seconds = 194 days. This ensures that most users will have become active at least once during this period.
This implies a length of SEQ1 in bits = 19.

Start conditions: Choose $SQN_{HE} = 0$ for all users and GLC = 1.

Arrival rate temporarily higher than clock rate: Choose $D = 2^{16}$.
D may be chosen quite large as long as the conditions in C.1.1.1 (4)(ii) and (iii) are satisfied. Choosing $D = 2^{16} = 65536$ means that the condition in C.1.1.1 (4)(i) is satisfied unless more than 65536 requests for batches arrive within over 18 hours which is practically impossible.

Verification of sequence numbers in the USIM:

This follows the handling of sequence numbers in the USIM specified in Annex C.2.

Length of the array: a = 32.
This satisfies the requirement in section 6.3.2 that the mechanism for the verification of sequence numbers shall ensure that a sequence number can still be accepted if it is among the last x sequence numbers generated.

Protection against wrap around: Choose $\Delta = 2^{28}$.
Choosing $\Delta = 2^{28}$ means that an attack to force the counter in the USIM to wrap around would require at least $SEQmax/\Delta = 2^{15} > 32.000$ successful authentications (cf. note 6 of C.2.3). We have $\Delta > p$, as required in note 7 of C.2.3.

Age limit for sequence numbers:
The use of such a limit is optional. The choice of a value for the parameter L affects only the USIM. It has no impact on the choice of other parameters and it entirely up to the operator, depending on his security policy. Therefore no particular value is suggested here. To give an example: if the policy stipulates that authentication vectors older than x seconds shall be rejected then L has to be set to x as the time unit of the clock is 1 second.

User anonymity: the value of SQN does not allow to trace the user over longer periods. Therefore, there may be no need to conceal SQN by an anonymity key as specified in section 6.3.

C.3.2 Profile 2: management of sequence numbers which are not time-based

Generation of sequence numbers:

This follows the scheme for the generation of sequence numbers specified in Annex C.1.1.2. The following parameter values are suggested for reference:

Length of IND in bits = 5.

Start conditions: $SQN_{HE} = 0$ for all users.

Verification of sequence numbers in the USIM:

Length of the array: a = 32

Protection against wrap around: Choose $\Delta = 2^{28}$.
Choosing $\Delta = 2^{28}$ means that an attack to force the counter in the USIM to wrap around would require at least $SEQmax/\Delta = 2^{15} > 32.000$ successful authentications (cf. note 6 of C.2.3). Note 7 of Annex C.2.3 does not apply.

Age limit for sequence numbers:
There is no clock here. So, the "age" limit would be interpreted as the maximum allowed difference between SQN_{MS} (see section 6.3) and the sequence number received. The use of such a limit is optional. The choice of a value for the parameter L affects only the USIM. It has no impact on the choice of other parameters and it entirely up to the operator, depending on his security policy. Therefore no particular value is suggested here.

User anonymity: the value of SQN may allow to trace the user over longer periods. If this is a concern then SQN has to be concealed by an anonymity key as specified in section 6.3.

C.3.3 Profile 3: management of sequence numbers which are entirely time-based

Generation of sequence numbers:

This follows the scheme for the generation of sequence numbers specified in Annex C.1.1.3. The following parameter values are suggested for reference:

Time unit of the clock: It has to be chosen in such a way that no two requests for a batch of authentication vectors arrive during one time unit. Value = 0.1 seconds

Length of IND in bits = 5.

Start conditions: GLC = 1 and, for all users, DIF = 0.

Verification of sequence numbers in the USIM:

This is done according to the handling of sequence numbers in the USIM specified in Annex C.2.

Length of the array: a = 32.
This satisfies the requirement in section 6.3.2 that the mechanism for the verification of sequence numbers shall ensure that a sequence number can still be accepted if it is among the last x sequence numbers generated.

Protection against wrap around: Choose $\Delta = 2^{28}$.
Choosing $\Delta = 2^{28}$ means that an attack to force the counter in the USIM to wrap around would require at least $SEQmax/\Delta = 2^{15} > 32.000$ successful authentications (cf. note 6 of C.2.3). Note 7 of C.2.3 does not apply.

Age limit for sequence numbers:
The use of such a limit is optional. The choice of a value for the parameter L affects only the USIM. It has no impact on the choice of other parameters and it entirely up to the operator, depending on his security policy. Therefore no particular value is suggested here. To give an example: if the policy stipulates that authentication vectors older than x time units shall be rejected then L has to be set to x.

User anonymity: the value of SQN does not allow to trace the user over longer periods. Therefore, there may be no need to conceal SQN by an anonymity key as specified in section 6.3.

C.3.4 Guidelines for the allocation of the index values in the array scheme

- **General rule**: index values *IND* used in the array scheme, according to Annex C.1.2, shall be allocated cyclically within its range 0, … , *a-1*. This means that the index value *IND* used with the previously generated authentication vector is stored in SQN_{HE}, and the next authentication vector shall use index value $IND + 1 \bmod a$.

It may be useful to allow exceptions to this general rule when additional information is available. This includes:

- Authentication vectors distributed within the same batch shall have the same index value.

  The Authentication Data Request MAP message contains information about the domain type (CS or PS) of the requesting serving node from which the request originates. It is recommended to use this information in the following way. Support for this use is, however, not required for an implementation to claim compliance to Annex C.

- Authentication vectors distributed to different service domains shall have different index values (i.e. separate ranges of index values are reserved for PS and CS operation).

In future releases there may be additional information about the requesting node identity. If this information is available it is recommended to use it in the following way:

- If the new request comes from the same serving node as the previous request, then the index value used for the new request shall be the same as was used for the previous request.

C.4 Guidelines for interoperability in a multi-vendor environment

The specification of a sequence number management scheme affects only the USIM and the AuC which are both under the control of one operator. Therefore, the specification of such a scheme is entirely at the discretion of an operator. Nevertheless, certain operators may not want to define a scheme of their own. Instead, they may want to rely on vendors implementing one of the schemes according to the profiles in C.3 or variants thereof. If these operators have multiple vendors for USIMs and/or AuCs, and the operators wish to move subscribers from the AuC of one vendor to that supplied by another one implementing a different scheme then this will work smoothly only when the following guidelines are adhered to by all the sequence number management schemes implemented in the operator's domain.

- The array mechanism specified in clauses C.1.2 and C.2 is used in the USIM to verify SQNs. The length of the IND used by the USIM to index the array shall be not less than the length of the IND used by the AuC when allocating index values. However, it is recommended that the same IND length of 5 bits is used in USIMs and AuCs. This is the same IND length as proposed for all profiles in clause C.3.

- Relation to Annex F: if the AMF field is used to signal further parameters relevant to sequence number management (age limit L) then the formats of the AMF and its interpretation by the USIM must be the same for all implementations in the operator's domain.

- Δ is larger than a specified minimum.
  This is necessary to accommodate schemes as in C.3.2 according to note 7 of C.2.3.
  We propose $\Delta \geq 2^{28}$.

- There are no requirements on the synchronicity of clocks in different AuCs for the time-based schemes. For the entirely time-based scheme, the following is recommended when moving users from one AuC to another one: The DIF value is updated in an appropriate manner when moving subscribers from an AuC to another AuC. More specifically, assume a user is moved from AuC1 to AuC2. If AuC1 is of profile 3 and AuC2 is of any profile then AuC1 sends GLC+DIF as SEQ_HE to AuC2. In the receiving end, if AuC2 is of profile 3 while AuC1 is of any profile then AuC2 sets DIF value for this user as DIF = SEQ_HE - GLC.

Annex D:
Void

Annex E:
Void

Annex F (informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the value received in an accepted network authentication token.

F.2 Changing sequence number verification parameters

This mechanism is used in conjunction with the mechanism for the verification of sequence number freshness in the USIM described in C.2.2.

The USIM shall also be able to put a limit L on the difference between SEQ_{HS} (the highest SEQ accepted so far) and a received sequence number SEQ. A mechanism to change this parameter L dynamically is useful since the optimum for these parameters may change over time. AMF is used to indicate a new value of L to be used by the USIM.

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.

Annex G (informative): Change history

Change history					
TSG SA #	Version	CR	Tdoc SA	New Version	Subject/Comment
SP-03	2.0.0	-	-	3.0.0	Approved at SA#3 and placed under TSG SA Change Control
SP-11	3.7.0	135	SP-010131	3.8.0	RES has to be a multiple of 8 bits
SP-11	3.7.0	136	SP-010131	3.8.0	Add bit ordering convention
SP-11	3.7.0	137	SP-010131	3.8.0	Timing of security mode procedure
SP-11	3.7.0	140	SP-010131	3.8.0	Correction to the handling of re-transmitted authentication request messages on the ME
SP-11	3.7.0	141	SP-010131	3.8.0	Optional Support for USIM-ME interface for GSM-Only ME
SP-11	3.7.0	142	SP-010131	3.8.0	Definition corrections
SP-11	3.7.0	143	SP-010131	3.8.0	GSM ciphering capability Handling in Security Mode set up procedure
SP-11	3.8.0	138	SP-010132	4.0.0	Add requesting node type to authentication data request
SP-11	3.8.0	139	SP-010132	4.0.0	Provide additional information to HE to detect fraud conditions.
SP-12	4.0.0	145	SP-010313	4.1.0	Correction to periodic local authentication
SP-12	4.0.0	147	SP-010314	4.1.0	Correction to COUNT-C description
SP-12	4.0.0	150	SP-010316	4.1.0	Calculation and Wrap-around of START value
SP-12	4.0.0	152	SP-010317	4.1.0	Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted
SP-12	4.0.0	154	SP-010319	4.1.0	THRESHOLD Check at RRC connection establishment
SP-13	4.1.0	155r1	SP-010492	4.2.0	Removing the list of access type codes from authentication failure report
SP-14	4.2.0	157	SP-010608	4.3.0	Annex F.2 (changing list parameters) modification
SP-14	4.2.0	159	SP-010609	4.3.0	Sequence Number Management Corrections
SP-14	4.2.0	161	SP-010610	4.3.0	SQN_{MS} retrieval in AuC during resynchronisation
SP-16	4.3.0	166	SP-020340	4.4.0	Optional use of Access Link Data Confidentiality
SP-16	4.3.0	170r1	SP-020342	4.4.0	Encryption/Integrity algorithms ordered by preference in Security Mode command
SP-16	4.3.0	172	SP-020343	4.4.0	Correction of (U)SIM toolkit security reference
SP-16	4.4.0	174r1	SP-020385	5.0.0	Clarification of sequence number management (Rel-5 created)